IP8800/S4600

トラブルシューティングガイド

IP88S46-T001-20

マニュアルはよく読み，保管してください。
・製品を使用する前に，安全上の説明を読み，十分理解してください。
・このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■対象製品

このマニュアルは IP8800/S4600 を対象に記載しています。

■輸出時の注意

本製品を輸出される場合には，外国為替及び外国貿易法の規制ならびに米国の輸出管理規則など外国の輸出関連法規をご確認のうえ，必要な手続きをお取りください。なお，不明な場合は，弊社担当営業にお問い合わせください。

■商標一覧

Cisco は，米国 Cisco Systems, Inc. の米国および他の国々における登録商標です。
Ethernet は，富士ゼロックス株式会社の登録商標です。
GSRP は，アラクサラネットワークス株式会社の登録商標です。
Internet Explorer は，米国 Microsoft Corporation の米国及びその他の国における登録商標または商標です。
IPX は，Novell,Inc. の商標です。
Microsoft は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
RSA，RSA SecurID は，RSA Security Inc. の米国およびその他の国における商標または登録商標です。
sFlow は，米国およびその他の国における米国 InMon Corp. の登録商標です。
UNIX は，The Open Group の米国ならびに他の国における登録商標です。
VitalQIP，VitalQIP Registration Manager は，アルカテル・ルーセントの商標です。
VLANaccessClient は，NEC ソフトの商標です。
Windows は，米国 Microsoft Corporation の米国およびその他の国における登録商標または商標です。
イーサネットは，富士ゼロックス株式会社の登録商標です。
そのほかの記載の会社名，製品名は，それぞれの会社の商標もしくは登録商標です。

■マニュアルはよく読み，保管してください。

製品を使用する前に，安全上の説明をよく読み，十分理解してください。
このマニュアルは，いつでも参照できるよう，手近な所に保管してください。

■ご注意

このマニュアルの内容については，改良のため，予告なく変更する場合があります。
また，出力表示例や図は，実際と異なる部分がある場合がありますのでご了承ください。

■発行

２０１５年　２月　(第３版)　ＩＰ８８Ｓ４６－Ｔ００１－２０

■著作権

変更履歴

【第 3 版】

表　変更履歴

項目	追加・変更内容
はじめに	• Ver.11.12 対応に伴い，「Ver.11.11.C より前のソフトウェアでご使用時の注意事項」を削除しました。
付録 A　show tech-support コマンド表示内容詳細	• 表示内容詳細にコマンドを追加しました。

なお，単なる誤字・脱字などはお断りなく訂正しました。

【第 2 版】

表　変更履歴

項目	追加・変更内容
はじめに	•「Ver.11.11.C より前のソフトウェアでご使用時の注意事項」の記述を変更しました。
装置障害におけるトラブルシュート	• 装置障害の対応手順の記述を変更しました。
運用中機能障害におけるトラブルシュート	•「認証 VLAN 使用時の通信障害」は認証 VLAN 未サポートのため削除しました。

はじめに

■対象製品

このマニュアルは IP8800/S4600 を対象に記載しています。

操作を行う前にこのマニュアルをよく読み，書かれている指示や注意を十分に理解してください。また，このマニュアルは必要なときにすぐ参照できるよう使いやすい場所に保管してください。

■このマニュアルの訂正について

このマニュアルに記載の内容は，「マニュアル訂正資料」で訂正する場合があります。

■対象読者

IP8800/S4600 を利用したネットワークシステムを構築し，運用するシステム管理者の方を対象としています。

また，次に示す知識を理解していることを前提としています。

- ネットワークシステム管理の基礎的な知識

■このマニュアルの URL

このマニュアルの内容は下記 URL に掲載しておりますので，あわせてご利用ください。

http://jpn.nec.com/ip88n/

■マニュアルの読書手順

本装置の導入，セットアップ，日常運用までの作業フローに従って，それぞれの場合に参照するマニュアルを次に示します。

- 装置の開梱から，初期導入時の基本的な設定について知りたい

クイックスタートガイド
(IP88S46-Q001)

- ハードウェアの設備条件，取扱方法について調べる

ハードウェア取扱説明書
(IP88S46-H001)

- ソフトウェアの機能，
コンフィグレーションの設定，
運用コマンドについて知りたい

- コンフィグレーションコマンドの 入力シンタックス，
パラメータ詳細について知りたい

コンフィグレーション コマンドレファレンス
Vol.1
(IP88S46-S004)

コンフィグレーション コマンドレファレンス
Vol.2
(IP88S46-S005)

- 運用コマンドの入力シンタックス，パラメータ詳細について知りたい

運用コマンドレファレンス
Vol.1
(IP88S46-S006)

運用コマンドレファレンス
Vol.2
(IP88S46-S007)

- メッセージとログについて調べる

メッセージ・ログレファレンス
(IP88S46-S008)

- トラブル発生時の対処方法について知りたい

トラブルシューティングガイド
(IP88S46-T001)

- MIB について調べる

MIB レファレンス
(IP88S46-S009)

■このマニュアルでの表記

AC	Alternating Current
ACK	ACKnowledge
ADSL	Asymmetric Digital Subscriber Line
ALG	Application Level Gateway
ANSI	American National Standards Institute

ARP	Address Resolution Protocol
AS	Autonomous System
AUX	Auxiliary
BCU	Basic Control Unit
BGP	Border Gateway Protocol
BGP4	Border Gateway Protocol - version 4
BGP4+	Multiprotocol Extensions for Border Gateway Protocol - version 4
bit/s	bits per second *bpsと表記する場合もあります。
BPDU	Bridge Protocol Data Unit
BRI	Basic Rate Interface
BSU	Basic Switching Unit
CC	Continuity Check
CDP	Cisco Discovery Protocol
CFM	Connectivity Fault Management
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common and Internal Spanning Tree
CLNP	ConnectionLess Network Protocol
CLNS	ConnectionLess Network System
CONS	Connection Oriented Network System
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSNP	Complete Sequence Numbers PDU
CST	Common Spanning Tree
CSU	Control and Switching Unit
DA	Destination Address
DC	Direct Current
DCE	Data Circuit terminating Equipment
DHCP	Dynamic Host Configuration Protocol
DIS	Draft International Standard/Designated Intermediate System
DNS	Domain Name System
DR	Designated Router
DSAP	Destination Service Access Point
DSCP	Differentiated Services Code Point
DTE	Data Terminal Equipment
DVMRP	Distance Vector Multicast Routing Protocol
E-Mail	Electronic Mail
EAP	Extensible Authentication Protocol
EAPOL	EAP Over LAN
EFM	Ethernet in the First Mile
ES	End System
FAN	Fan Unit
FCS	Frame Check Sequence
FDB	Filtering DataBase
FQDN	Fully Qualified Domain Name
FTTH	Fiber To The Home
GBIC	GigaBit Interface Converter
GSRP	Gigabit Switch Redundancy Protocol
HMAC	Keyed-Hashing for Message Authentication
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICMPv6	Internet Control Message Protocol version 6
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers, Inc.
IETF	the Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPCP	IP Control Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPV6CP	IP Version 6 Control Protocol
IPX	Internetwork Packet Exchange
ISO	International Organization for Standardization
ISP	Internet Service Provider
IST	Internal Spanning Tree
L2LD	Layer 2 Loop Detection
LAN	Local Area Network
LCP	Link Control Protocol
LED	Light Emitting Diode
LLC	Logical Link Control
LLDP	Link Layer Discovery Protocol
LLPQ	Low Latency Priority Queueing
LLQ+3WFQ	Low Latency Queueing + 3 Weighted Fair Queueing

```
LLRLQ      Low Latency Rate Limited Queueing
LSP        Label Switched Path
LSP        Link State PDU
LSR        Label Switched Router
MA         Maintenance Association
MAC        Media Access Control
MC         Memory Card
MD5        Message Digest 5
MDI        Medium Dependent Interface
MDI-X      Medium Dependent Interface crossover
MEP        Maintenance association End Point
MIB        Management Information Base
MIP        Maintenance domain Intermediate Point
MRU        Maximum Receive Unit
MSTI       Multiple Spanning Tree Instance
MSTP       Multiple Spanning Tree Protocol
MSU        Management and Switching Unit
MTU        Maximum Transfer Unit
NAK        Not AcKnowledge
NAS        Network Access Server
NAT        Network Address Translation
NCP        Network Control Protocol
NDP        Neighbor Discovery Protocol
NET        Network Entity Title
NIF        Network Interface
NLA ID     Next-Level Aggregation Identifier
NPDU       Network Protocol Data Unit
NSAP       Network Service Access Point
NSSA       Not So Stubby Area
NTP        Network Time Protocol
OADP       Octpower Auto Discovery Protocol
OAM        Operations,Administration,and Maintenance
OSPF       Open Shortest Path First
OUI        Organizationally Unique Identifier
packet/s   packets per second     *ppsと表記する場合もあります。
PAD        PADding
PAE        Port Access Entity
PC         Personal Computer
PCI        Protocol Control Information
PDU        Protocol Data Unit
PICS       Protocol Implementation Conformance Statement
PID        Protocol IDentifier
PIM        Protocol Independent Multicast
PIM-DM     Protocol Independent Multicast-Dense Mode
PIM-SM     Protocol Independent Multicast-Sparse Mode
PIM-SSM    Protocol Independent Multicast-Source Specific Multicast
PoE        Power over Ethernet
PRI        Primary Rate Interface
PS         Power Supply
PSNP       Partial Sequence Numbers PDU
PSP        Packet Switching Processor
QoS        Quality of Service
QSFP+      Quad Small Form factor Pluggable Plus
RA         Router Advertisement
RADIUS     Remote Authentication Dial In User Service
RDI        Remote Defect Indication
REJ        REJect
RFC        Request For Comments
RGQ        Rate Guaranteed Queueing
RIP        Routing Information Protocol
RIPng      Routing Information Protocol next generation
RMON       Remote Network Monitoring MIB
RPF        Reverse Path Forwarding
RQ         ReQuest
RSTP       Rapid Spanning Tree Protocol
SA         Source Address
SD         Secure Digital
SDH        Synchronous Digital Hierarchy
SDU        Service Data Unit
SEL        NSAP SELector
SFD        Start Frame Delimiter
SFP        Small Form factor Pluggable
SFP+       Enhanced Small Form factor Pluggable
SMTP       Simple Mail Transfer Protocol
```

SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNP	Sequence Numbers PDU
SNPA	Subnetwork Point of Attachment
SOP	System Operational Panel
SPF	Shortest Path First
SSAP	Source Service Access Point
STP	Spanning Tree Protocol
TA	Terminal Adapter
TACACS+	Terminal Access Controller Access Control System Plus
TCP/IP	Transmission Control Protocol/Internet Protocol
TLA ID	Top-Level Aggregation Identifier
TLV	Type, Length, and Value
TOS	Type Of Service
TPID	Tag Protocol Identifier
TTL	Time To Live
UDLD	Uni-Directional Link Detection
UDP	User Datagram Protocol
UPC	Usage Parameter Control
UPC-RED	Usage Parameter Control - Random Early Detection
uRPF	unicast Reverse Path Forwarding
VAA	VLAN Access Agent
VLAN	Virtual LAN
VNI	VXLAN Network Identifier
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding/Virtual Routing and Forwarding Instance
VRRP	Virtual Router Redundancy Protocol
VTEP	Virtual Tunnel End Point
VXLAN	Virtual eXtensible Local Area Network
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queueing
WGQ	Weighted Guaranteed Queueing
WRED	Weighted Random Early Detection
WS	Work Station
WWW	World-Wide Web
XFP	10 gigabit small Form factor Pluggable

■ kB(バイト) などの単位表記について

1kB(キロバイト), 1MB(メガバイト), 1GB(ギガバイト), 1TB(テラバイト) はそれぞれ 1024 バイト, 1024^2 バイト, 1024^3 バイト, 1024^4 バイトです。

目次

1 概要

この章では，障害解析の概要について説明します。

1.1　障害解析概要

このマニュアルは，本装置に問題がある場合に利用してください。

装置を目視で直接確認する場合は「1.2　装置および装置一部障害解析概要」に沿って解析を進めてください。

装置にログインして確認する場合は「1.3　機能障害解析概要」に沿って解析を進めてください。

1.2　装置および装置一部障害解析概要

運用中に障害が発生し，装置を目視で直接確認できる場合には，「2.1　IP8800/S4600 のトラブルシュート」の対策内容に従ってトラブルシュートしてください。

装置の LED については「図 1-1　正面パネルのレイアウトの例」「表 1-1　LED の表示，スイッチ，コネクタ」に示します。

なお，オプション機構（NIF，電源機構，ファンユニット）の LED などの情報や，「図 1-1　正面パネルのレイアウトの例」に示した以外の正面パネルのレイアウトについては，「ハードウェア取扱説明書」を参照してください。

また，装置を目視で直接確認できない場合でも，リモート運用端末から運用コマンドで装置の LED を確認することにより，装置を目視できる場合と同様にトラブルシュートすることができます。

図 1-1　正面パネルのレイアウトの例

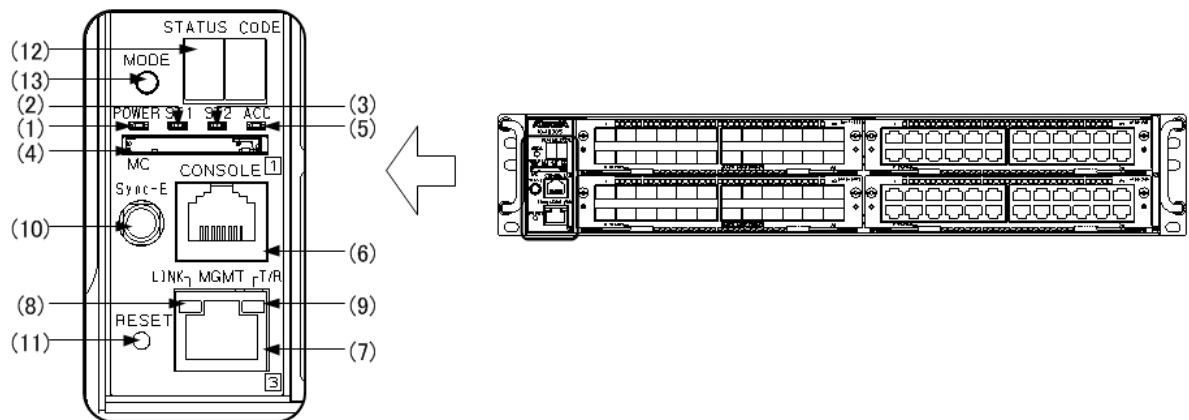



表 1-1　LED の表示，スイッチ，コネクタ

番号	名称	種類	状態	内容	
1	POWER	LED: 緑	電源の投入状態を示す。	緑点灯	電源 ON
				消灯	電源 OFF，または電源異常
2	ST1	LED: 緑 / 橙 / 赤	装置の状態を示す。	緑点灯	動作可能
				緑点滅	準備中（立上げ中）
				橙点灯	電源投入時の初期状態。
				赤点滅	装置の部分障害発生
				赤点灯	装置の致命的障害発生（継続使用不可）
				消灯	電源 OFF，または電源異常
3	ST2	LED：緑 / 橙	スタック構成時のマスタスイッチ / スタック準備中を示す。	緑点灯	マスタスイッチとして動作
				橙点灯	電源投入時の初期状態

番号	名称	種類	状態	内容	
				消灯	電源 OFF，スタック準備中，またはスタンドアロンとして動作
4	MC	コネクタ	メモリカードスロット	メモリカードスロット	
5	ACC	LED: 緑	メモリカードの状態	点灯	メモリカードアクセス中 （メモリカード取り外し禁止）
				消灯	メモリカードアイドル中 （メモリカード取り付け，取り外し可能）
6	CONSOLE	コネクタ	CONSOLE ポート	コンソール端末接続用 RS-232C ポート	
7	MGMT	コネクタ	MANAGEMENT ポート	装置管理用ネットワークインタフェース 10/100/1000BASE-T AutoMDI/MDIX	
8	LINK	LED: 緑	MANAGEMENT ポートの動作状態を示す。	緑点灯	電源投入時の初期状態，またはリンク確立
				消灯	ST1 LED が緑点灯の場合，リンク障害，または閉塞
9	T/R	LED: 緑		緑点滅	フレーム送受信中
				消灯	送受信フレームなし
10	Sync-E	コネクタ	（未使用）	（未使用）	
11	RESET	スイッチ （ノンロック）	装置のマニュアルリセットスイッチ	装置を再起動する	
12	STATUS CODE	7seg.LED：緑	スタック構成時の装置番号を示す。	緑点灯	スタック構成時，装置番号を表示 （例：０１）
				消灯	装置起動時，またはスタンドアロン状態
13	MODE	スイッチ （ノンロック）	（未使用）	（未使用）	

（凡例）－：該当なし

1.3 機能障害解析概要

本装置の機能障害解析概要を次の表に示します。

なお，上位レイヤの通信障害は，下位レイヤの通信障害が原因の場合があるので，下位レイヤの項目も確認してください。

表 1-2 機能障害の状況と参照個所

大項目	中項目	参照個所
ログインパスワードを忘れた	ログインユーザのパスワード忘れ	3.1.1 ログインユーザのパスワードを忘れてしまった
	装置管理者モード変更のパスワード忘れ	3.1.2 装置管理者モード変更のパスワードを忘れてしまった
MC のトラブル	"MC : --------" と表示された	3.2.1 show system コマンドまたは show mc コマンドで "MC : --------" と表示される
	"MC not found." と表示された	3.2.2 MC へのアクセス時に "MC not found." と表示される
	MC へのアクセスができなかった	3.2.3 MC へのアクセスができなかった
運用端末のトラブル	コンソール入力・表示不可	3.3.1 コンソールからの入力，表示がうまくできない
	リモートログインできない	3.3.2 リモート運用端末からログインできない
	装置管理者モードに戻れない	3.3.3 コンフィグレーションコマンドモードから装置管理者モードに戻れない
	ログイン認証不可	3.3.4 RADIUS/TACACS+ を利用したログイン認証ができない
	コマンド承認不可	3.3.5 RADIUS/TACACS+/ ローカルを利用したコマンド承認ができない
スタック構成のトラブル	スタックを構成できない	3.4.1 スタックを構成できない
	スタック構成でコンフィグレーションが編集できない	3.4.2 スタック構成でコンフィグレーションが編集できない
	マスタスイッチを固定してスタックを構成したい	3.4.3 特定のメンバスイッチをマスタスイッチにしてスタックを構成したい
ネットワークインタフェースの通信障害	イーサネットポートの通信障害	3.5.1 イーサネットポートの接続ができない
	10BASE-T/100BASE-TX/ 1000BASE-T の通信障害	3.5.2 10BASE-T/100BASE-TX/1000BASE-T のトラブル発生時の対応
	100BASE-FX/1000BASE-X の通信障害	3.5.3 100BASE-FX/1000BASE-X のトラブル発生時の対応
	10GBASE-R の通信障害	3.5.4 10GBASE-R/40GBASE-R のトラブル発生時の対応
	リンクアグリゲーションでの障害	3.5.5 リンクアグリゲーション使用時の通信障害
レイヤ 2 ネットワークの通信障害	VLAN 障害	3.6.1 VLAN によるレイヤ 2 通信ができない
	スパニングツリー障害	3.6.2 スパニングツリー機能使用時の障害
	Ring Protocol 障害	3.6.3 Ring Protocol 機能使用時の障害
	IGMPsnooping 不可	3.6.4 IGMP snooping によるマルチキャスト中継ができない

大項目	中項目	参照個所
	MLDsnooping 不可	3.6.5 MLD snooping によるマルチキャスト中継ができない
IPv4 ネットワークの通信障害	通信ができない	3.7.1 通信できない，または切断されている
	DHCP が機能しない	3.7.2 DHCP 機能で IP アドレスが割り振られない
	DynamicDNS が動かない	3.7.3 DHCP 機能で DynamicDNS 連携が動作しない
IPv4 ユニキャストルーティングの通信障害	RIP 情報なし	3.8.1 RIP 経路情報が存在しない
	OSPF 情報なし	3.8.2 OSPF 経路情報が存在しない
	BGP4 情報なし	3.8.3 BGP4 経路情報が存在しない
	VRF 情報なし	3.8.4 VRF で IPv4 経路情報が存在しない
IPv4 マルチキャストルーティングの通信障害	PIM-SM ネットワークで通信不可	3.9.1 IPv4 PIM-SM ネットワークで通信ができない
	PIM-SM ネットワークでデータが二重中継された	3.9.2 IPv4 PIM-SM ネットワークでマルチキャストデータが二重中継される
	PIM-SSM ネットワークで通信不可	3.9.3 IPv4 PIM-SSM ネットワークで通信ができない
	PIM-SSM ネットワークでデータが二重中継された	3.9.4 IPv4 PIM-SSM ネットワークでマルチキャストデータが二重中継される
	VRF での通信の不具合	3.9.5 VRF での IPv4 マルチキャスト通信のトラブル
	エクストラネットの通信障害	3.9.6 エクストラネットでの IPv4 マルチキャスト通信のトラブル
IPv6 ネットワークの通信障害	通信できない	3.10.1 通信できない，または切断されている
	DHCP リレーの不具合	3.10.2 IPv6 DHCP リレーの通信トラブル
	DHCP サーバの不具合	3.10.3 IPv6 DHCP サーバに関するトラブルシューティング
IPv6 ユニキャストルーティングの通信障害	RIPng の情報がない	3.11.1 RIPng 経路情報が存在しない
	OSPFv3 の情報がない	3.11.2 OSPFv3 経路情報が存在しない
	BGP4+ の情報がない	3.11.3 BGP4+ 経路情報が存在しない
	VRF の情報がない	3.11.4 VRF で IPv6 経路情報が存在しない
IPv6 マルチキャストルーティングの通信障害	PIM-SM ネットワークで通信不可	3.12.1 IPv6 PIM-SM ネットワークで通信ができない
	PIM-SM ネットワークでデータが二重中継された	3.12.2 IPv6 PIM-SM ネットワークでマルチキャストデータが二重中継される
	PIM-SSM ネットワークで通信不可	3.12.3 IPv6 PIM-SSM ネットワークで通信ができない
	PIM-SSM ネットワークでデータが二重中継された	3.12.4 IPv6 PIM-SSM ネットワークでマルチキャストデータが二重中継される
	VRF での通信の不具合	3.12.5 VRF での IPv6 マルチキャスト通信のトラブル
	エクストラネットの通信障害	3.12.6 エクストラネットでの IPv6 マルチキャスト通信のトラブル

大項目	中項目	参照個所
レイヤ 2 認証の通信障害	IEEE802.1X で認証できない	3.13.1　IEEE 802.1X 使用時の通信障害
	Web 認証で認証できない	3.13.2　Web 認証使用時の通信障害
	MAC 認証で認証できない	3.13.3　MAC 認証使用時の通信障害
GSRP の障害	ー	3.14.1　GSRP の通信障害
IPv4 の VRRP 障害	ー	3.14.2　IPv4 ネットワークの VRRP 構成で通信ができない
IPv6 の VRRP 障害	ー	3.14.3　IPv6 ネットワークの VRRP 構成で通信ができない
アップリンク・リダンダント機能障害	ー	3.14.4　アップリンク・リダンダント構成で通信ができない
SNMP の通信障害	MIB が取得できない	3.15.1　SNMP マネージャから MIB の取得ができない
	トラップ受信不可	3.15.2　SNMP マネージャでトラップが受信できない
sFlow 統計の障害	sFlow パケットが届かない	3.16.1　sFlow パケットがコレクタに届かない
	フローサンプルが届かない	3.16.2　フローサンプルがコレクタに届かない
	カウンタサンプルが届かない	3.16.3　カウンタサンプルがコレクタに届かない
LLDP 機能で隣接装置情報が取れない	ー	3.17.1　LLDP 機能により隣接装置情報が取得できない
OADP 機能で隣接装置情報が取れない	ー	3.17.2　OADP 機能により隣接装置情報が取得できない
NTP の通信障害	ー	3.18.1　NTP による時刻同期ができない
IEEE802.3ah/UDLD 機能使用時の障害	ポートが inactive 状態になる	3.19.1　IEEE802.3ah/UDLD 機能でポートが inactive 状態となる
省電力機能のトラブル	スケジュールが動作しない	3.20.1　スケジュールが動作しない
パケット廃棄による通信障害	ー	3.22.1　フィルタ /QoS 設定情報の確認
DHCP snooping のトラブル	ー	3.23　DHCP snooping のトラブル
ポリシーベースルーティングのトラブル	指定した経路に中継されない	3.24.1　ポリシーベースルーティングで中継されない場合の確認方法
	トラック状態が想定と異なる	3.24.2　ポリシーベースルーティングのトラッキング機能でトラック状態が想定と異なる場合の確認方法
その他	ー	マニュアル「コンフィグレーションガイド」によって，再度設定を確認してください

2 装置障害におけるトラブルシュート

この章では，装置に障害が発生した場合の対処方法を説明します。

2.1　IP8800/S4600 のトラブルシュート

2.1.1　装置障害の対応手順

装置に障害が発生した場合には，以下の手順で対応します。

表 2-1　装置障害のトラブルシュート

項番	障害内容	対策内容
1	• 装置から発煙している • 装置から異臭が発生している • 装置から異常音が発生している	直ちに次の手順を実行してください。 1. 装置の電源を OFF にします。 （AC 電源の場合には装置の電源ケーブルを抜きます。） 上記の手順で運用を停止後，販売店に連絡してください。
2	login プロンプトが表示されない	1. MC が挿入されている場合は，MC を抜いた上で装置の電源を OFF にし，再度 ON にして装置を再起動します。 2. MC が挿入されていない場合は，装置の電源を OFF にし，再度 ON にして装置を再起動します。 3. 装置を再起動させても問題が解決しない場合には，装置を交換します。
3	装置正面の PWR LED が消灯している	1. 電源機構の LED を確認し，以下の手順を実施します。 （1）ALARM LED が赤点灯している電源機構があれば，電源機構を交換します。 （2）POWER LED および ALARM LED の両方が消灯している電源機構があれば，「表 2-2　電源障害の確認事項」を実施します。問題が解決しない場合には，LED が消灯している電源機構を交換します。 （3）上記 (1)(2) に該当しない場合は，装置をを再起動して環境に異常がないかを確認します。 （4）装置を再起動できた場合は，show logging コマンドを実行して障害情報を確認します。 >show logging | grep ERR （5）採取した障害情報に " 高温注意 " のメッセージが存在する場合には，動作環境が原因と考えられるため，システム管理者に環境の改善を依頼します。 （6）装置を再起動できない場合，上記（5）の手順で障害情報が存在しないまたは " 高温注意 " のメッセージが存在しない場合は，装置に障害が発生しているため，装置を交換してください。 2. 電源機構がすべて正常に動作している場合には，装置を交換します。
4	装置正面の ST1 LED が赤点灯している	1. 装置に障害が発生しています。 （1）show logging コマンドを実行して障害情報を確認します。 >show logging | grep ERR （2）採取した障害情報を「メッセージログ・レファレンス」を参照して，記載されている対応を実施してください。 （3）上記 (2) の対応後も ST1LED が赤点灯している場合は，装置を交換してください。

項番	障害内容	対策内容
5	装置正面の ST1 LED が赤点滅している	1. 電源機構の LED を確認します。 （1）ALARM LED が赤点灯している電源機構がある場合は，電源機構を交換します。 （2）POWER LED および ALARM LED の両方が消灯している電源機構がある場合は「表 2-2　電源障害の確認事項」を実施します。問題が解決しない場合には，LED が消灯している電源機構を交換します。 （3）すべての電源機構が正常に動作している場合は，電源機構をそのままの状態で保持します。 （4）上記 (1)(2) に該当しない場合は，show logging コマンドを実行して障害情報を確認します。 >show logging	grep ERR （5）採取した障害情報に "FAN 障害 " のメッセージが存在する場合は，該当 FAN ユニットを交換してください。 （6）採取した障害情報に "NIF ボード障害 " のメッセージが存在する場合は，該当 NIF ボードを交換してください。

表 2-2　電源障害の確認事項

項番	確認事項	対応内容
1	電源設備のブレーカを OFF になっている	電源設備のブレーカを OFF にします。
2	• 電源ケーブルが抜けている • 電源ケーブルがしっかりと取り付けられていない	次の手順を実施してください。 1. 電源設備のブレーカを OFF にします。 2. 電源ケーブルを正しく取り付けます。 3. 電源設備のブレーカを ON にします。
3	電源機構がしっかり取り付けられていなくて，がたついている	次の手順を実施してください。 1. 電源設備のブレーカを OFF にします。 2. 電源ケーブルを取り外します。 3. 電源機構を取り外し，しっかりと挿入します。 4. 電源ケーブルを取り付けます。 5. 電源設備のブレーカを ON にします。
4	測定した入力電源が以下の範囲外である AC100V の場合：AC90 ～ 132V AC200V の場合：AC180 ～ 264V 注　本件は入力電源の測定が可能な場合だけ実施する	設備担当者に連絡して入力電源の対策を依頼してください。

2.1.2 装置およびオプション機構の交換方法

装置およびオプション機構の交換方法は，「ハードウェア取扱説明書」に記載されています。記載された手順に従って実施してください。

3 運用中機能障害におけるトラブルシュート

本章では装置が正常に動作しない，または通信ができないといったトラブルが発生した場合の対処方法を説明します。

3.1 ログインパスワードのトラブル

3.1.1 ログインユーザのパスワードを忘れてしまった

ログインユーザのパスワードを忘れて本装置にログインできない場合は，次に示す方法で対応してください。

- ログインできるユーザがほかにいる場合
  ログインできるユーザが，装置管理者モードで password コマンドを実行しパスワードを忘れたログインユーザのパスワードを再設定します。または，clear password コマンドでパスワードを削除します。これらのコマンドは，装置管理者モードで実行します。したがって，ログインするユーザは入力モードを装置管理者モードに変更するための enable コマンドのパスワードを知っている必要があります。
  パスワードを忘れた user1 のパスワードを管理者モードで再設定する例を次の図に示します。

図 3-1　user1 のパスワードを再設定する例

```
# password user1
Changing local password for user1.
New password:
Retype new password:
#
```

- ログインできるユーザがいない場合
  ログインできるユーザがいない場合，またはログインできても enable コマンドのパスワードがわからない場合，本体のリセットスイッチを 5 秒以上押して，デフォルトリスタートをします。デフォルトリスタートによる起動のあと，パスワードを再設定してください。
  デフォルトリスタートで起動したあとは，パスワードによるログイン認証，装置管理者モードへの変更（enable コマンド）時の認証，およびコマンド承認をしないため，十分に注意してください。
  デフォルトリスタートについては，マニュアル「コンフィグレーションガイド」を参照してください。

なお，再設定したパスワードは装置を再起動したあと，有効になります。

3.1.2 装置管理者モード変更のパスワードを忘れてしまった

enable コマンドのパスワードを忘れて，入力モードを装置管理者モードに変更できない場合，本体のリセットスイッチを 5 秒以上押して，デフォルトリスタートをします。デフォルトリスタートによる起動のあと，パスワードを再設定してください。

デフォルトリスタートで起動したあとは，パスワードによるログイン認証，装置管理者モードへの変更（enable コマンド）時の認証，およびコマンド承認をしないため，十分に注意してください。

デフォルトリスタートについては，マニュアル「コンフィグレーションガイド」を参照してください。

なお，再設定したパスワードは装置を再起動したあと，有効になります。

3.2 MC のトラブル

3.2.1 show system コマンドまたは show mc コマンドで "MC : --------" と表示される

show system コマンドまたは show mc コマンドで "MC : --------" と表示される場合は，次の表に従って確認してください。

表 3-1 "MC : --------" と表示される場合の対応方法

項番	確認内容・コマンド	対応
1	ACC LED を確認してください。	ACC LED が緑点灯の場合は，他プロセスが MC にアクセス中の可能性があります。ACC LED が消灯後，再度コマンドを実行してください。 ACC LED が緑点灯でない場合は，項番 2 へ。
2	一度 MC を抜いて，再度挿入してください。	MC の抜き差し後，再度コマンドを実行してください。 MC を挿入する際には，MC および装置のメモリカードスロットにほこりが付着していないか確認してください。ほこりが付着しているときは，乾いた布などでほこりを取ってから MC を挿入してください。 MC の抜き差しを数回繰り返しても現象が改善しない場合は，項番 3 へ。
3	MC を交換してください。	MC を交換後，再度コマンドを実行してください。 MC を交換しても現象が改善しない場合は，メモリカードスロットが故障している可能性があります。 装置を交換してください。

3.2.2 MC へのアクセス時に "MC not found." と表示される

MC へアクセスするコマンドの実行時に "MC not found." と表示される場合は，次の表に従って確認してください。

表 3-2 "MC not found." と表示される場合の対応方法

項番	確認内容・コマンド	対応
1	ACC LED を確認してください。	ACC LED が緑点灯の場合は，他プロセスが MC にアクセス中の可能性があります。ACC LED が消灯後，再度コマンドを実行してください。 ACC LED が緑点灯でない場合は，項番 2 へ。
2	一度 MC を抜いて，再度挿入してください。	MC の抜き差し後，再度コマンドを実行してください。 MC を挿入する際には，MC および装置のメモリカードスロットにほこりが付着していないか確認してください。ほこりが付着しているときは，乾いた布などでほこりを取ってから MC を挿入してください。 MC の抜き差しを数回繰り返しても現象が改善しない場合は，項番 3 へ。
3	MC を交換してください。	MC を交換後，再度コマンドを実行してください。 MC を交換しても現象が改善しない場合は，メモリカードスロットが故障している可能性があります。 装置を交換してください。

3.2.3 MC へのアクセスができなかった

MC へアクセスするコマンドの実行に失敗した場合は，次の表に従って確認してください。

表 3-3 MC へアクセスができなかった場合の対応方法

項番	確認内容・コマンド	対応
1	対象の MC が弊社推奨のものか確認してください。	弊社推奨の MC でない場合は，正しくアクセスできない可能性があります。 弊社推奨の MC の場合は，項番 2 へ。
2	本装置で MC がフォーマットされたか確認してください。	弊社推奨の MC を他装置（PC など）でフォーマットした場合は，正しくアクセスできない可能性があります。本装置に MC を挿入し，運用コマンド format mc を実行してフォーマットしてください。 本装置で MC をフォーマットしても現象が改善しない場合は，項番 3 へ。
3	MC を交換してください。	MC を交換後，再度コマンドを実行してください。 MC を交換しても現象が改善しない場合は，メモリカードスロットが故障している可能性があります。 装置を交換してください。

3.3 運用端末のトラブル

3.3.1 コンソールからの入力，表示がうまくできない

コンソールとの接続トラブルが発生した場合は，「表 3-4　コンソールとの接続トラブルおよび対応」に従って確認してください。

モデムとの接続トラブルが発生した場合には，「表 3-5　モデムとの接続トラブルおよび対応」に従って確認してください。また，モデムに付属している取扱説明書を参照してください。

表 3-4　コンソールとの接続トラブルおよび対応

項番	障害内容	確認内容
1	画面に何も表示されない	次の手順で確認してください。 1. 装置の正面パネルにある ST1 LED が緑点灯になっているかを確認してください。緑点灯していない場合は，「1.2　装置および装置一部障害解析概要」を参照してください。 2. ケーブルの接続が正しいか確認してください。 3. RS232C クロスケーブルを用いていることを確認してください。 4. ポート番号，通信速度，データ長，パリティビット，ストップビット，フロー制御などの通信ソフトウェアの設定が以下のとおりになっているか確認してください。 通信速度：9600bit/s（変更している場合は設定値） データ長：8bit パリティビット：なし ストップビット：1bit フロー制御：なし
2	キー入力を受け付けない	次の手順で確認してください。 1. XON ／ XOFF によるフロー制御でデータの送受信を中断している可能性があります。データ送受信の中断を解除してください（[Ctrl] ＋ [Q] をキー入力してください)。それでもキー入力ができない場合は 2. 以降の確認をしてください。 2. 通信ソフトウェアの設定が正しいか確認してください。 3. [Ctrl] ＋ [S] によって画面が停止している可能性があります。何かキーを入力してください。
3	異常な文字が表示される	通信ソフトウェアとのネゴシエーションが正しくできていない可能性があります。通信ソフトウェアの通信速度を次の手順で確認してください。 1. コンフィグレーションコマンド line console 0 で CONSOLE(RS232C) の通信速度を設定していない場合は，通信ソフトウェアの通信速度が 9600bit/s に設定されているか確認してください。 2. コンフィグレーションコマンド line console 0 で CONSOLE(RS232C) の通信速度を 1200，2400，4800，9600，または 19200bit/s に設定している場合は，通信ソフトウェアの通信速度が正しく設定されているか確認してください。
4	ユーザ名入力中に異常な文字が表示された	CONSOLE(RS232C) の通信速度を変更された可能性があります。項番 3 を参照してください。
5	ログインできない	1. 画面にログインプロンプトが出ているか確認してください。出ていなければ，装置を起動中のため，しばらくお待ちください。 2. コンフィグレーションコマンド aaa authentication login console および aaa authentication login で，RADIUS/TACACS+ 認証が設定されていないか確認してください（詳細は「3.3.4　RADIUS/TACACS+ を利用したログイン認証ができない」を参照してください)。
6	ログイン後に通信ソフトウェアの通信速度を変更したら異常な文字が表示され，コマンド入力ができない	ログイン後に通信ソフトウェアの通信速度を変更しても正常な表示はできません。通信ソフトウェアの通信速度を元に戻してください。

項番	障害内容	確認内容
7	Tera Term Pro を使用してログインしたいがログイン時に異常な文字が表示される	通信ソフトウェアとのネゴシエーションが正しくできていない可能性があります。項番 3 を参照してください。［Alt］＋［B］でブレーク信号を発行します。なお，Tera Term Pro の通信速度によって，複数回ブレーク信号を発行しないとログイン画面が表示されないことがあります。
8	項目名と内容がずれて表示される	1 行で表示可能な文字数を超える情報を表示している可能性があります。通信ソフトウェアの設定で画面サイズを変更し，1 行で表示可能な文字数を多くしてください。

表 3-5 モデムとの接続トラブルおよび対応

項番	障害内容	確認内容
1	モデムが自動着信しない	次のことを確認してください。 • ケーブルの接続が正しいこと。 • モデムの電源が ON になっていること。 • 電話番号が正しいこと。 • モデムの設定内容が正しいこと。 • 2 台の端末にモデムを接続し，ダイアルすることで回線接続できること。
2	ログイン時に異常な文字が表示される	次の手順で確認してください。 1. モデムの通信速度を 9600bit/s に設定してください。 2. モデムが V.90，K56flex，x2 またはそれ以降の通信規格に対応している場合は，V.34 通信方式以下で接続するように設定してください。
3	回線切断後，再ダイアルしても通話中でつながらない	回線が切断されてから数秒間は着信しない場合があります。モデムのマニュアルを参照してください。
4	回線障害後，再接続できない	障害によって回線が切断された場合，最大 120 秒間は再接続できないことがあります。すぐに接続したい場合は別手段でログインし，AUX にダイアルアップ IP 接続をしているユーザを killuser コマンドで強制ログアウトさせてください。
5	回線切断後，再接続できない	ダイアルアップ IP 接続が切断された場合，すぐに再接続できないことがあります。その場合，300 秒間程度の間隔を空けてから再接続してください。

3.3.2 リモート運用端末からログインできない

リモート運用端末との接続トラブルが発生した場合は，次の表に従って確認をしてください。

表 3-6 リモート運用端末との接続トラブルおよび対応

項番	現象	対処方法，または参照個所
1	リモート接続ができない。	次の手順で確認してください。 1. PC や WS から ping コマンドを使用してリモート接続のための経路が確立されているかを確認してください。 2. コネクション確立のメッセージ表示後プロンプトが表示されるまで時間がかかる場合は，DNS サーバとの通信ができなくなっている可能性があります（DNS サーバとの通信ができない場合プロンプトが表示されるまで約 5 分かかります。なお，この時間は目安でありネットワークの状態によって変化します）。

項番	現象	対処方法，または参照個所
2	ログインができない。	次の手順で確認してください。 1. コンフィグレーションコマンド line vty モードのアクセスリストで許可された IP または IPv6 アドレスを持つ端末を使用しているかを確認してください。また，コンフィグレーションコマンドアクセスリストで設定した IP または IPv6 アドレスに deny を指定していないかを確認してください（詳細はマニュアル「コンフィグレーションガイド」を参照してください）。 2. ログインできる最大ユーザ数を超えていないか確認してください（詳細はマニュアル「コンフィグレーションガイド」を参照してください）。 なお，最大ユーザ数でログインしている状態でリモート運用端末から本装置への到達性が失われ，その後復旧している場合，TCP プロトコルのタイムアウト時間が経過しセッションが切断されるまで，リモート運用端末からは新たにログインできません。TCP プロトコルのタイムアウト時間はリモート運用端末の状態やネットワークの状態によって変化しますが，おおむね 10 分です。 3. コンフィグレーションコマンド line vty モードの transport input で，本装置へのアクセスを禁止しているプロトコルを使用していないか確認してください（詳細はマニュアル「コンフィグレーションコマンドレファレンス」を参照してください）。 4. コンフィグレーションコマンド aaa authentication login で，RADIUS/TACACS+ 認証が設定されていないか確認してください（詳細は「3.3.4 RADIUS/TACACS+ を利用したログイン認証ができない」を参照してください）。
3	キー入力を受け付けない。	次の手順で確認してください。 1. XON ／ XOFF によるフロー制御でデータの送受信を中断している可能性があります。データ送受信の中断を解除してください（［Ctrl］＋［Q］をキー入力してください）。それでもキー入力できない場合は，項番 2 以降の確認をしてください。 2. 通信ソフトウェアの設定が正しいか確認してください。 3. ［Ctrl］＋［S］によって画面が停止している可能性があります。何かキーを入力してください。
4	ログインしたままの状態になっているユーザがある。	自動ログアウトするのを待つか，再度ログインしてログインしたままの状態になっているユーザを killuser コマンドで削除します。また，コンフィグレーションを編集中の場合は，コンフィグレーションの保存がされていないなど編集中の状態になっているので，再度ログインしてコンフィグレーションモードになってから保存するなどしたのち，編集を終了してください。

3.3.3　コンフィグレーションコマンドモードから装置管理者モードに戻れない

コンフィグレーションコマンドモードから装置管理者モードに戻れなくなった場合は，次に示す方法で対応してください。

(1)　コンソールとの接続時

次の手順で，該当するユーザを強制的にログアウトさせてください。

1. show sessions コマンドで，該当するユーザのログイン番号を確認します。

［実行例］

```
(config)# $show sessions
operator console admin 1 Jan 6 14:16
                         ↑ 該当するユーザのログイン番号
```

2. killuser コマンドで，該当するユーザを強制的にログアウトさせます。
<login no.> パラメータには，手順 1. で調べたログイン番号を指定してください。

[実行例]

```
(config)# $killuser 1
```

(2) リモート運用端末との接続時

いったんリモート運用端末を終了させたあと，再接続してください。

ログインしたままの状態になっているユーザがある場合は，「表 3-6　リモート運用端末との接続トラブルおよび対応」の項番 4 に従って対処してください。

3.3.4　RADIUS/TACACS+ を利用したログイン認証ができない

RADIUS ／ TACACS+ を利用したログイン認証ができない場合，以下の確認を行ってください。

1. RADIUS ／ TACACS+ サーバへの通信
   ping コマンドで，本装置から RADIUS ／ TACACS+ サーバに対して疎通ができているかを確認してください。疎通ができない場合は，「3.7.1　通信できない，または切断されている」を参照してください。また，コンフィグレーションでローカルアドレスを設定している場合は，ローカルアドレスから ping コマンドで，本装置から RADIUS ／ TACACS+ サーバに対して疎通ができているかを確認してください。

2. タイムアウト値およびリトライ回数設定
   RADIUS 認証の場合，コンフィグレーションコマンド radius-server host，radius-server retransmit，radius-server timeout の設定によって，本装置が RADIUS サーバとの通信が不能と判断する時間は最大で＜設定したタイムアウト値 (秒) ＞×＜設定したリトライ回数＞×＜設定した RADIUS サーバ数＞となります。
   TACACS+ 認証の場合，コンフィグレーションコマンド tacacs-server host，tacacs-server timeout の設定によって，本装置が TACACS+ サーバとの通信が不能と判断する時間は最大で < 設定したタイムアウト値 (秒)> × < 設定した TACACS+ サーバ数＞となります。この時間が極端に大きくなると，リモート運用端末の telnet などのアプリケーションがタイムアウトによって終了する可能性があります。この場合，RADIUS ／ TACACS+ コンフィグレーションの設定かリモート運用端末で使用するアプリケーションのタイムアウトの設定を変更してください。また，運用ログに RADIUS ／ TACACS+ 認証が成功したメッセージが出力されているにもかかわらず，telnet や ftp が失敗する場合は，コンフィグレーションで指定した複数の RADIUS サーバの中で，稼働中の RADIUS ／ TACACS+ サーバに接続するまでに，リモート運用端末側のアプリケーションがタイムアウトしていることが考えられるため，稼働中の RADIUS ／ TACACS+ サーバを優先するように設定するか，＜タイムアウト値 (秒) ＞×＜リトライ回数＞の値を小さくしてください。

3. 本装置にログインできない場合の対処方法
   設定ミスなどで本装置にログインできない場合は，コンソールからログインして修正してください。なお，コンフィグレーションコマンド aaa authentication login console によって，コンソールもログイン認証の対象となっている場合は，デフォルトリスタート後，ログインして修正してください。

   デフォルトリスタート

   本体のリセットスイッチを 5 秒以上押します。
   パスワードによるログイン認証，装置管理者モードへの変更（enable コマンド）時の認証，およびコマンド承認をしないため，デフォルトリスタートで起動する場合は十分に注意してください。
   なお，設定したパスワードは装置を再起動したあと，有効になります。

3.3.5　RADIUS/TACACS+/ ローカルを利用したコマンド承認ができない

RADIUS ／ TACACS+ ／ローカル認証は成功して本装置にログインできたが，コマンド承認がうまくできない場合や，コマンドを実行しても承認エラーメッセージが表示されてコマンドが実行できない場合は，以下の確認を行ってください。

1. show whoami の確認
   本装置の show whoami コマンドで，現在のユーザが許可・制限されている運用コマンドのリストを表示・確認できます。RADIUS ／ TACACS+ サーバの設定どおりにコマンドリストが取得できていることを確認してください。また，ローカルコマンド承認を使用している場合は，コンフィグレーションどおりにコマンドリストが設定されていることを確認してください。

2. サーバ設定およびコンフィグレーションの確認
   RADIUS ／ TACACS+ サーバ側で，本装置のコマンド承認に関する設定が正しいことを確認してください。特に RADIUS の場合はベンダー固有属性の設定，TACACS+ の場合は Service と属性名などに注意してください。また，ローカルコマンド承認を使用している場合は，コンフィグレーションの設定が正しいことを確認してください。RADIUS ／ TACACS+ ／ローカル（コンフィグレーション）の設定については，マニュアル「コンフィグレーションガイド」を参照してください。
   コマンドリスト記述時の注意
   本装置のコマンド承認用のコマンドリストを記述する際には空白の扱いに注意してください。例えば，許可コマンドリストに”show ip　”(show ip の後にスペース) が設定してある場合は，show ip interface コマンドは許可されますが，show ipv6 interface コマンドは制限されます。

3. コマンドがすべて制限された場合の対処方法
   設定ミスなどでコマンドがすべて制限された場合は，コンソールからログインして修正してください。なお，コンフィグレーションコマンド aaa authorization commands console によって，コンソールもコマンド承認の対象となっている場合は，デフォルトリスタート後，ログインして修正してください。
   デフォルトリスタート
   本体のリセットスイッチを 5 秒以上押します。
   パスワードによるログイン認証，装置管理者モードへの変更（enable コマンド）時の認証，およびコマンド承認をしないため，デフォルトリスタートで起動する場合は十分に注意してください。
   なお，設定したパスワードは装置を再起動したあと，有効になります。

3.4 スタック構成のトラブル

3.4.1 スタックを構成できない

スタックを正常に構成できない場合は，メンバスイッチの状態，オプションライセンスの情報，スタックポートの状態の順に確認してください。

1. ログの確認
   ログは，マニュアル「メッセージ・ログレファレンス」を参照してください。
2. メンバスイッチの状態，オプションライセンス情報，スタックポートの状態による原因の切り分け
   次の表に従って原因の切り分けを行ってください。

表 3-7 スタックを構成できない場合の対応方法

項番	確認内容・コマンド	対応
1	各メンバスイッチで次のコマンドを実行して，メンバスイッチの状態を確認してください。 show switch detail	Stack status が Disable の場合，スタンドアロンで動作中です。 コンフィグレーションコマンド stack enable を設定して，スタートアップコンフィグレーションへ保存したあと装置を再起動して，スタック機能を動作させてください。
		Switch No がメンバスイッチ間で重複している場合，スタックを構成できません。 set switch コマンドでスイッチ番号を変更して，メンバスイッチ間でスイッチ番号が重複しないようにしてください。なお，set switch コマンドによるスイッチ番号の変更を有効にするには，メンバスイッチの再起動が必要です。
		上記に該当しない場合は項番 2 へ。
2	各メンバスイッチで次のコマンドを実行して，メンバスイッチのオプションライセンス情報を確認してください。 show license	各メンバスイッチに設定しているオプションライセンスが一致していない場合，スタックを構成できません。 set license コマンドまたは erase license コマンドを使用し，メンバスイッチ間でオプションライセンスを一致させてください。なお，これらのコマンドで適用したライセンスキーを有効にするには，メンバスイッチの再起動が必要です。
		上記に該当しない場合は項番 3 へ。
3	各メンバスイッチで次のコマンドを実行して，スタックポートの状態を確認してください。 show port show switch detail	show port コマンドの実行結果で，Status が up ではない場合，「3.5.1 イーサネットポートの接続ができない」を参照して，イーサネットポートの状態を確認してください。
		show port コマンドの実行結果で Status が up の場合，かつ show switch コマンドに detail パラメータを指定した実行結果で Status が Down の場合，スタックポートで接続しているメンバスイッチ間で，コンフィグレーションが誤っているおそれがあります。 次に示すコンフィグレーションを確認してください。 • スタックポートの設定 コンフィグレーションコマンド switchport mode の stack パラメータで設定されたスタックポートが，実際に接続しているポートと異なっていないか確認します。

3.4.2 スタック構成でコンフィグレーションが編集できない

スタックを構成できてもコンフィグレーションが編集できない場合，ソフトウェア情報を確認してください。

マスタスイッチで“`remote command all show version`”を実行して，スタックを構成するすべての

メンバスイッチのソフトウェア情報を確認します。次に示すソフトウェア情報が一致していないと，スタックを構成できてもコンフィグレーションが編集できません。

- ソフトウェア種別（OS-L3CA または OS-L3CL）
- ソフトウェアバージョン

一致していなかった場合は，スタックを構成するすべてのメンバスイッチでソフトウェア情報を一致させてください。

3.4.3 特定のメンバスイッチをマスタスイッチにしてスタックを構成したい

マスタスイッチにしたいメンバスイッチのマスタ選出優先度に大きな値を設定して，スタックを構成するすべてのメンバスイッチを同時に起動（または再起動）しても，マスタ選出優先度の大きなメンバスイッチがマスタスイッチにならないことがあります。これは，次に示す要因などによって起動に掛かる時間が変わり，各メンバスイッチの起動するタイミングがずれてしまうためです。

- 再起動による起動である
- ソフトウェア種別やソフトウェアバージョンが異なる
- スタートアップコンフィグレーションが異なる
- 起動前にソフトウェアをアップデートまたはアップグレードした

マスタスイッチとなるメンバスイッチを固定したい場合は，次のどちらかの方法でスタックを構成してください。

- マスタスイッチにしたいメンバスイッチを先に起動してください。このメンバスイッチが起動してマスタスイッチとなったことを確認したあとで，残りのメンバスイッチを起動してください。
- マスタスイッチにしたいメンバスイッチのマスタ選出優先度を 2 以上に設定して，残りのメンバスイッチのマスタ選出優先度を 1 に設定してください。その後，すべてのメンバスイッチを起動してください。

3.5　ネットワークインタフェースの通信障害

3.5.1　イーサネットポートの接続ができない

通信障害の原因がイーサネットポートにあると考えられる場合は，次に示す手順で確認してください。

NIF の状態，ポートの状態，ポートの統計情報の順に確認してください。

(1) NIF の状態確認

1. ログの確認
   ログは，マニュアル「メッセージ・ログレファレンス」を参照してください。
2. NIF の状態による原因の切り分け
   show nif コマンドによって NIF 状態を確認し，次の表に従って原因の切り分けを行ってください。

表 3-8　NIF 状態の確認および対応

項番	NIF 状態	原因	対応
1	active	該当 NIF は正常に動作中です。	「表 3-9　ポート状態の確認および対応」によってポートの状態を確認してください。
2	notconnect	該当 NIF が実装されていません。	NIF を実装してください。 NIF を実装する場合は，装置電源を OFF にしてから実施してください。
3	fault	該当 NIF が障害となっています。	show logging コマンドによって表示される該当 NIF のログより，マニュアル「メッセージ・ログレファレンス」の該当個所を参照し，記載されている［対応］に従って対応してください。
4	initialize	該当 NIF が初期化中です。	初期化が完了するまで待ってください。
5	disable	電源投入後に NIF が挿入されている，または本装置でサポートされていない NIF が実装されています。	NIF を交換してください。 NIF を交換する場合は，装置電源を OFF にしてから実施してください。

(2) ポートの状態確認

1. ログの確認
   ログは，マニュアル「メッセージ・ログレファレンス」を参照してください。
2. ポートの状態による原因の切り分け
   show interfaces コマンドによってポート状態を確認し，次の表に従って原因の切り分けを行ってください。

表 3-9　ポート状態の確認および対応

項番	ポート状態	原因	対応
1	active up	該当ポートは正常に動作中です。	なし

項番	ポート状態	原因	対応
2	active down	該当ポートに回線障害が発生しています。	• 光ケーブルまたはトランシーバ（ダイレクトアタッチケーブルを含む）が半挿しになっている可能性があります。光ケーブルまたはトランシーバをいったん外して，再度接続してください。 • 上記に該当しない場合は，show logging コマンドによって表示される該当ポートのログより，マニュアル「メッセージ・ログレファレンス」の該当個所を参照し，記載されている［対応］に従って対応してください。
3	inactive	下記のどれかによって inactive 状態となっています。 • inactivate コマンド • リンクアグリゲーションのスタンバイリンク機能 • スパニングツリーの BPDU ガード機能 • GSRP のポートリセット機能 • IEEE802.3ah/UDLD 機能での障害検出 • L2 ループ検知機能によってポートを inactive 状態にした • ストームコントロール機能によってポートを inactive 状態にした	• リンクアグリゲーションのスタンバイリンク機能によって inactive 状態になっている場合は，正常な動作なので，activate コマンドで active 状態にしないでください。スタンバイリンク機能は show channel-group コマンドで detail パラメータを指定し確認してください。 • スパニングツリーの BPDU ガード機能によって inactive 状態になっている場合は，対向装置の設定を見直し，本装置で BPDU を受信しない構成にし，activate コマンドで該当ポートを active 状態にしてください。BPDU ガード機能は show spanning-tree コマンドで detail パラメータを指定し確認してください。 • GSRP のポートリセット機能によって inactive 状態になっている場合は，自動的に active 状態に戻ります。正常な動作なので，activate コマンドで active 状態にしないでください。 • IEEE802.3ah/UDLD 機能で片方向リンク障害または L2 ループが検出されたことによって inactive 状態になっている場合は，「3.19　IEEE802.3ah/UDLD 機能の通信障害」を参照してください。障害復旧後，activate コマンドで該当ポートを active 状態にしてください。 • L2 ループ検知機能によって inactive 状態になっている場合は，ループが発生する構成を変更した後，activate コマンドで該当ポートを active 状態にしてください。また，コンフィグレーションコマンドで loop-detection auto-restore-time が設定されている場合は，自動的に active 状態に戻ります。 • ストームコントロール機能によって inactive 状態になっている場合は，LAN がストームから回復後，activate コマンドで該当ポートを active 状態にしてください。 • 上記のどれでもない場合に，active 状態にしたいときは，使用するポートにケーブルが接続されていることを確認の上，activate コマンドで該当ポートを active 状態にしてください。
4	test	test interfaces コマンドによって，該当ポートは回線テスト中です。	通信を再開する場合は，no test interfaces コマンドで回線テストを停止後，activate コマンドで該当ポートを active 状態にしてください。
5	fault	該当ポートのポート部分のハードウェアが障害となっています。	show logging コマンドによって表示される該当ポートのログより，マニュアル「メッセージ・ログレファレンス」の該当個所を参照し，記載されている［対応］に従って対応してください。
6	initialize	該当ポートが初期化中です。	初期化が完了するまで待ってください。
7	disable または locked	コンフィグレーションコマンド shutdown が設定されています。	使用するポートにケーブルが接続されていることを確認の上，コンフィグレーションコマンドで no shutdown を設定して該当ポートを active 状態にしてください。

(3) 統計情報の確認

show port statistics コマンドを実行し，本装置に実装されている全ポートの送受信パケット数，送受信廃

棄パケット数を確認できます。

図 3-2 「ポートの動作状況確認」表示例

```
> show port statistics
Date 20XX/01/14 10:56:37 UTC
Port Counts: 84
Port  Name           Status T/R  All packets   Multicast   Broadcast     Discard
 0/ 1 ftygeth1/0/1   down   Tx   41601114258 32945109231           1           0
                            Rx    6352088724       15118           8           0
 0/ 2 ftygeth1/0/2   down   Tx             0           0           0           0
                            Rx             0           0           0           0
 0/ 3 ftygeth1/0/3   up     Tx  230169902708 25895910148      557807           0
                            Rx   34671538289       66885     1487508           0
 0/ 4 ftygeth1/0/4   down   Tx   42422843302 41973185821         160           0
                            Rx    5839856540        5593       42399           0
 1/ 1 geth1/1/1      up     Tx         36060       36012          48           0
                            Rx  267868905982 67868905982           0           0
 1/ 2 geth1/1/2      down   Tx             0           0           0           0
                            Rx             0           0           0           0
 1/ 3 geth1/1/3      down   Tx             0           0           0           0
                            Rx             0           0           0           0
(以下省略)
>
```

なお，本コマンド実行時に表示項目 "Discard" の表示が 0 より大きい場合は，パケットが廃棄される障害が発生しています。show interfaces コマンドで該当ポートの詳細情報を取得してください。

3.5.2 10BASE-T/100BASE-TX/1000BASE-T のトラブル発生時の対応

10BASE-T/100BASE-TX/1000BASE-T でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. ログの確認
   ログは，マニュアル「メッセージ・ログレファレンス」を参照してください。
2. 障害解析方法に従った原因の切り分け
   次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-10 10BASE-T/100BASE-TX/1000BASE-T のトラブル発生時の障害解析方法

項番	確認内容	原因	対応
1	show interfaces コマンドの障害統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Link down	回線品質が低下しています。	ケーブルの種別が正しいか確認してください。種別は「ハードウェア取扱説明書」を参照してください。
			本装置の設定が次の場合はピンマッピングが MDI-X であるか確認してください。 • 該当ポートの設定が固定接続となっている場合 • 該当ポートの設定がオートネゴシエーションかつ自動 MDIX 機能を無効にしている場合
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。
			本装置でサポートしている接続インタフェースに交換してください。本装置でサポートしている接続インタフェースについては，マニュアル「コンフィグレーションガイド」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces（イーサネット）コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1 回線をテストする」を参照してください。

項番	確認内容	原因	対応
2	show interfaces コマンドの受信系エラー統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • CRC errors • Symbol errors	回線品質が低下しています。	ケーブルの種別が正しいか確認してください。種別は「ハードウェア取扱説明書」を参照してください。
			本装置の設定が次の場合はピンマッピングが MDI-X であるか確認してください。 • 該当ポートの設定が固定接続となっている場合 • 該当ポートの設定がオートネゴシエーションかつ自動 MDIX 機能を無効にしている場合
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。
			本装置でサポートしている接続インタフェースに交換してください。本装置でサポートしている接続インタフェースについては，マニュアル「コンフィグレーションガイド」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1　回線をテストする」を参照してください。
3	show interfaces コマンドの障害統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • MDI cross over changed	ケーブルのピンマッピングが不正です。	ピンマッピングを正しく直してください。ピンマッピングについては，マニュアル「コンフィグレーションガイド」を参照してください。
4	show interfaces コマンドのポート detail 情報によって該当ポートで回線種別 / 回線速度を確認してください。不正な回線種別 / 回線速度の場合，原因と対応欄を参照してください。	ケーブルが適合していません。	ケーブルの種別が正しいか確認してください。種別は「ハードウェア取扱説明書」を参照してください。
		コンフィグレーションコマンド speed と duplex が相手装置と不一致です。	コンフィグレーションコマンド speed と duplex を相手装置と合わせてください。
		上記以外の場合。	オートネゴシエーションで特定の速度を使用したい場合は，オートネゴシエーションの回線速度を設定してください。詳細は，マニュアル「コンフィグレーションガイド」を参照してください。
5	show interfaces コマンドの障害統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Long frames	受信できるフレーム長を超えたパケットを受信しています。	ジャンボフレームの設定を相手装置と合わせてください。
6	show qos queueing コマンドで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • discard_pkt	パケットの廃棄が発生しています。	廃棄制御およびシェーパのシステム運用が適切であるかを見直してください。

3.5.3　100BASE-FX/1000BASE-X のトラブル発生時の対応

100BASE-FX/1000BASE-X でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. ログの確認
   ログについては，マニュアル「メッセージ・ログレファレンス」を参照してください。
2. 障害解析方法に従った原因の切り分け
   次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-11　100BASE-FX/1000BASE-X のトラブル発生時の障害解析方法

項番	確認内容	原因	対応
1	show interfaces コマンドの障害統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Link down • Signal detect errors	受信側の回線品質が低下しています。	光ファイバの種別を確認してください。種別は「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			コンフィグレーションコマンド speed と duplex を相手装置と合わせてください。
			相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1　回線をテストする」を参照してください。
2	show interfaces コマンドの受信系エラー統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • CRC errors • Symbol errors	受信側の回線品質が低下しています。	光ファイバの種別を確認してください。モードは「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			コンフィグレーションコマンド speed と duplex を相手装置と合わせてください。
			相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。

項番	確認内容	原因	対応
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1　回線をテストする」を参照してください。
3	show interfaces コマンドの障害統計情報によって，該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • TX fault	トランシーバが故障しています。	トランシーバを交換してください。
4	1000BASE-BX などの 1 芯の光ファイバを使用している場合，相手側のトランシーバと組み合わせが合っているか確認してください。	トランシーバの組み合わせが不正です。	1000BASE-BX を使用する場合，トランシーバは U タイプと D タイプを対向して使用する必要があります。トランシーバの種別が正しいか確認してください。
5	100BASE-FX を使用している場合，show interfaces コマンドのポート detail 情報によって該当ポートで回線種別 / 回線速度を確認してください。不正な回線種別 / 回線速度の場合，原因と対応欄を参照してください。	コンフィグレーションコマンド speed と duplex が相手装置と不一致です。	コンフィグレーションコマンド speed と duplex を相手装置と合わせてください。
6	show interfaces コマンドの障害統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Long frames	受信できるフレーム長を超えたパケットを受信しています。	ジャンボフレームの設定を相手装置と合わせてください。
7	show qos queueing コマンドで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • discard_pkt	パケットの廃棄が発生しています。	廃棄制御およびシェーパのシステム運用が適切であるかを見直してください。

3.5.4　10GBASE-R/40GBASE-R のトラブル発生時の対応

10GBASE-R/40GBASE-R でトラブルが発生した場合は，以下の順序で障害の切り分けを行ってください。

1. ログの確認
   ログについては，マニュアル「メッセージ・ログレファレンス」を参照してください。
2. 障害解析方法に従った原因の切り分け
   次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-12 10GBASE-R/40GBASE-R のトラブル発生時の障害解析方法

項番	確認内容	原因	対応
1	show interfaces コマンドの障害統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Signal detect errors	受信側の回線品質が低下しています。	光ファイバの種別を確認してください。種別は「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			トランシーバを相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1　回線をテストする」を参照してください。
2	show interfaces コマンドの受信系エラー統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • CRC errors • Symbol errors	受信側の回線品質が低下しています。	光ファイバの種別を確認してください。種別は「ハードウェア取扱説明書」を参照してください。
			光アッテネータ（光減衰器）を使用している場合，減衰値を確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			ケーブル長を確認してください。ケーブル長は「ハードウェア取扱説明書」を参照してください。
			ケーブルの接続が正しいか確認してください。また，ケーブルの端面が汚れていないか確認してください。汚れている場合，汚れを拭き取ってください。
			トランシーバの接続が正しいか確認してください。
			トランシーバを相手装置のセグメント規格と合わせてください。
			光レベルが正しいか確認してください。光レベルは「ハードウェア取扱説明書」を参照してください。
			本装置の回線テストを実行して受信側機能に問題ないか確認してください。no test interfaces コマンドの実行結果を参照し，記載されている［対策］に従って対応してください。指定するテスト種別は「5.1　回線をテストする」を参照してください。
4	show interfaces コマンドの障害統計情報によって該当ポートで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • Long frames	受信できるフレーム長を超えたパケットを受信しています。	ジャンボフレームの設定を相手装置と合わせてください。

項番	確認内容	原因	対応
5	show qos queueing コマンドで以下の統計情報がカウントされていないか確認してください。カウントされている場合，原因と対応欄を参照してください。 • discard_pkt	パケットの廃棄が発生しています。	廃棄制御およびシェーパのシステム運用が適切であるかを見直してください。

3.5.5　リンクアグリゲーション使用時の通信障害

リンクアグリゲーション使用時に通信ができない，または縮退運転している場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-13　リンクアグリゲーション使用時の通信の障害解析方法

項番	確認内容・コマンド	対応
1	通信障害となっているリンクアグリゲーションの設定を，show channel-group コマンドで detail パラメータを指定して確認してください。	リンクアグリゲーションのモードが相手装置のモードと同じ設定になっているか確認してください。相手装置とモードが異なった場合，相手装置と同じモードに変更してください。
		リンクアグリゲーションのモードが一致している場合，各ポートの LACP 開始方法が両方とも passive になっていないか確認してください。両方とも passive になっていた場合，どちらか一方を active に変更してください。
2	通信障害となっているポートの運用状態を show channel-group コマンドで detail パラメータを指定して確認してください。	各ポートの状態（Status）を確認してください。チャネルグループ内の全ポートが Down の場合，チャネルグループが Down します。 Down ポートは Reason の表示によって以下を行ってください。 • CH Disabled チャネルグループが Disable 状態となって DOWN しています。 • Port Down リンクダウンしています。「3.5　ネットワークインタフェースの通信障害」を参照してください。 • Port Speed Unmatch チャネルグループ内の他ポートと回線速度が不一致となって縮退状態になっています。縮退を回避する場合はチャネルグループ内の全ポートの速度が一致するようにしてください。 • Port Selecting ポートアグリゲーション条件チェック実施中のため，縮退状態になっています。しばらく待っても回復しない場合は，相手装置の運用状態，および設定を確認してください。 • Waiting Partner Synchronization ポートアグリゲーション条件チェックを完了し接続ポートの同期待ちとなって縮退状態になっています。しばらく待っても回復しない場合は相手装置の運用状態の確認，および設定の確認をしてください。 • Partner System ID Unmatch 接続ポートから受信した Partner System ID がグループの Partner System ID と不一致となって縮退状態になっています。縮退を回避する場合は相手装置の運用状態の確認，配線の確認をしてください。

項番	確認内容・コマンド	対応
		• LACPDU Expired 接続ポートからの LACPDU 有効時刻を超過したため，該当ポートが縮退状態となっています。show channel-group statistics コマンドで lacp パラメータを指定し，LACPDU の統計情報を確認してください。また相手装置の運用状態の確認をしてください。 • Partner Key Unmatch 接続ポートから受信した Key がグループの Partner Key が不一致のため縮退状態となっています。縮退を回避する場合は相手装置の運用状態の確認，配線の確認をしてください。 • Partner Aggregation Individual 接続ポートからリンクアグリゲーション不可を受信したため縮退状態となっています。縮退を回避する場合は相手装置の運用状態の確認，および設定の確認をしてください。 • Partner Synchronization OUT_OF_SYNC 接続ポートから同期不可を受信したため縮退状態となっています（本装置でコンフィグレーションを変更した場合や相手装置で回線を inactive 状態にした場合に発生します)。 • Port Moved 接続されていたポートがほかのポートと接続しました。配線の確認をしてください。 • Operation of Detach Port Limit 離脱ポート数制限機能が動作したため，チャネルグループが Down しています。

3.6 レイヤ 2 ネットワークの通信障害

3.6.1 VLAN によるレイヤ 2 通信ができない

VLAN 使用時にレイヤ 2 通信ができない場合は，次に示す障害解析方法に従って原因の切り分けを行ってください。

(1) VLAN 状態の確認

show vlan コマンド，または show vlan コマンドを detail パラメータ指定で実行し，VLAN の状態を確認してください。以下に，VLAN 機能ごとの確認内容を示します。

(a) 全 VLAN 機能での共通確認

● ポートに VLAN を正しく設定しているか。

● ポートのモードの設定は合っているか。また，デフォルト VLAN（VLAN ID 1）で期待したポートが所属していない場合は，以下の設定を確認してください。
- VLAN ID 1 以外のポート VLAN をアクセス VLAN またはネイティブ VLAN に指定していないか。
- トランクポートで allowed vlan にデフォルト VLAN の設定が抜けていないか。
- ミラーポートに指定していないか。

● トランクポートに IEEE802.1X の VLAN 単位認証（静的），Web 認証（固定 VLAN モード），または MAC 認証を設定している VLAN と，設定していない VLAN を混在して設定していないか。

(b) プロトコル VLAN の場合の確認

プロトコル VLAN を使用している場合は，show vlan コマンドを実行して，プロトコルが正しく設定されていることを確認してください。

```
# show vlan
       :
VLAN ID:100   Type:Protocol based  Status:Up
  Protocol VLAN Information  Name:ipv4
    EtherType:0800,0806  LLC:  Snap-EtherType:
  Learning:On   Uplink-VLAN:       Uplink-Block:    Tag-Translation:
       :
```

(c) MAC VLAN の場合の確認

● MAC VLAN を使用している場合は，show vlan mac-vlan コマンドを実行して，VLAN で通信を許可する MAC アドレスが正しく設定されていることを確認してください。括弧内は，MAC アドレスの登録元機能を表しています。

［登録元機能］

static：コンフィグレーションによって設定された MAC アドレスです。

dot1x：IEEE802.1X によって設定された MAC アドレスです。

wa：Web 認証によって設定された MAC アドレスです。

```
# show vlan mac-vlan
       :
VLAN ID:100     MAC Counts:4
    0012.e200.0001 (static)        0012.e200.00:02 (static)
    0012.e200.0003 (static)        0012.e200.00:04 (dot1x)
```

● show vlan mac-vlan コマンドを実行して，レイヤ 2 認証機能とコンフィグレーションで同じ MAC アド

レスを異なる VLAN に設定していないことを確認してください。*（アスタリスク）が表示されている MAC アドレスは，コンフィグレーションで同じ MAC アドレスが設定され，無効になっていることを示します。

```
# show vlan mac-vlan
       :
VLAN ID:500     MAC Counts:4
    0012.e200.aa01 (static)        0012.e200.aa02 (static)
    0012.e200.aa03 (static)        0012.e200.aa04 (dot1x)
VLAN ID:600     MAC Counts:1
  * 0012.e200.aa01 (dot1x)
```

(2) ポート状態の確認

- show vlan コマンドを detail パラメータ指定で実行し，ポートが Up 状態であることを確認してください。Down 状態の場合は「3.5　ネットワークインタフェースの通信障害」を参照してください。
- ポートが Forwarding 状態であることを確認してください。Blocking 状態である場合は，括弧内の要因によって Blocking 状態となっています。要因となっている機能の運用状態を確認してください。

[要因]

VLAN : VLAN が suspend 指定です。
CH : リンクアグリゲーションによって転送停止中です。
STP : スパニングツリーによって転送停止中です。
GSRP : GSRP によって転送停止中です。
dot1x : IEEE802.1X によって転送停止中です。
CNF : コンフィグレーション設定不可のため転送停止中です。
AXRP : Ring Protocol によって転送停止中です。

```
# show vlan detail
       :
VLAN ID:100   Type:Protocol based  Status:Up
       :
  Port Information
   1/1/1         Up   Forwarding      Untagged
   1/4/1         Up   Forwarding      Tagged
```

(3) MAC アドレステーブルの確認

(a) MAC アドレス学習の状態の確認

- show mac-address-table コマンドを実行して，通信障害となっている宛先 MAC アドレスの情報を確認してください。

```
# show mac-address-table
MAC address         VLAN    Type     Port-list
0012.e22c.650c        10    Dynamic  1/1
0012.e22c.650b         1    Dynamic  1/2
```

- Type 表示によって以下の対処を行ってください。

【Type 表示が Dynamic の場合】

MAC アドレス学習の情報が更新されていない可能性があります。clear mac-address-table コマンドで古い情報をクリアしてください。宛先の装置からフレームを送信することでも情報を更新できます。

【Type 表示が Static の場合】

コンフィグレーションコマンド mac-address-table static で設定している転送先ポートを確認してください。

【Type 表示が Snoop の場合】

「3.6.4　IGMP snooping によるマルチキャスト中継ができない」および「3.6.5　MLD snooping によるマルチキャスト中継ができない」を参照してください。

【Type 表示が Dot1x の場合】

「3.13.1　IEEE 802.1X 使用時の通信障害」を参照してください。

【Type 表示が Wa の場合】

「3.13.2　Web 認証使用時の通信障害」を参照してください。

【Type 表示が Macauth の場合】

「3.13.3　MAC 認証使用時の通信障害」を参照してください。

● 該当する MAC アドレスが表示されない場合はフラッディングされます。
表示されないにもかかわらず通信ができない場合は，ポート間中継抑止が設定されていないか確認してください。また，ストームコントロール機能で閾値が小さい値になっていないか確認してください。

(4) フィルタ /QoS の確認

フィルタによって特定のパケットが廃棄されているか，または QoS 制御の帯域監視，廃棄制御もしくはシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築での帯域監視，廃棄制御またはシェーパのシステム運用が適切であるかを確認してください。手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

3.6.2 スパニングツリー機能使用時の障害

スパニングツリー機能を使用し，レイヤ 2 通信の障害，またはスパニングツリーの運用状態がネットワーク構成どおりでない場合，次の表に示す解析方法に従って原因の切り分けを行ってください。マルチプルスパニングツリーの場合は，CIST または MST インスタンスごとに確認をしてください。例えば，ルートブリッジに関して確認するときは，CIST のルートブリッジまたは MST インスタンスごとのルートブリッジと読み替えて確認してください。

表 3-14　スパニングツリーの障害解析方法

項番	確認内容・コマンド	対応
1	障害となっているスパニングツリーに対して show spanning-tree コマンドを実行し，スパニングツリーのプロトコル動作状況を確認してください。	Enable の場合は項番 2 へ。
		Ring Protocol と PVST+ を共存動作させているとき，対象 VLAN のツリー情報が表示されていない場合は項番 7 へ。
		Disable の場合はスパニングツリーが停止状態になっているためコンフィグレーションを確認してください。
		Ring Protocol とマルチプルスパニングツリーが共存動作している場合は項番 8 へ。
		PVST+ 数が収容条件内に収まっているかを確認してください。

項番	確認内容・コマンド	対応
2	障害となっているスパニングツリーに対して show spanning-tree コマンドを実行し，スパニングツリーのルートブリッジのブリッジ識別子を確認してください。	ルートブリッジのブリッジ識別子がネットワーク構成どおりのルートブリッジになっている場合は項番 3 へ。
		ルートブリッジのブリッジ識別子がネットワーク構成どおりのルートブリッジでない場合は，ネットワーク構成，コンフィグレーションを確認してください。
3	障害となっているスパニングツリーに対して show spanning-tree コマンドを実行し，スパニングツリーのポート状態，ポート役割を確認してください。	スパニングツリーのポート状態，ポート役割がネットワーク構成どおりになっている場合は項番 4 へ。
		スパニングツリーのポート状態，ポート役割がネットワーク構成とは異なる場合は，隣接装置の状態とコンフィグレーションを確認してください。
4	障害となっているスパニングツリーに対して show spanning-tree statistics コマンドを実行し，障害となっているポートで BPDU の送受信を確認してください。	BPDU の送受信カウンタを確認してください。 【ルートポートの場合】 BPDU 受信カウンタがカウントアップされている場合は項番 5 へ。 カウントアップされていない場合は，フィルタによって BPDU が廃棄されているか，または QoS 制御の帯域監視，廃棄制御もしくはシェーパによって BPDU が廃棄されている可能性があります。「3.22.1　フィルタ /QoS 設定情報の確認」を参照し，確認してください。問題がない場合は，隣接装置を確認してください。 【指定ポートの場合】 BPDU 送信カウンタがカウントアップされている場合は項番 5 へ。 カウントアップされていない場合は，「3.5　ネットワークインタフェースの通信障害」を参照してください。
5	障害となっているスパニングツリーに対して，show spanning-tree コマンドを detail パラメータ指定で実行し受信 BPDU のブリッジ識別子を確認してください。	受信 BPDU のルートブリッジ識別子，送信ブリッジ識別子がネットワーク構成どおりになっていることを確認してください。ネットワーク構成と異なっていた場合は隣接装置の状態を確認してください。
6	障害となっているスパニングツリーの最大数が収容条件内か確認してください。	収容条件の範囲内で設定してください。 収容条件については，マニュアル「コンフィグレーションガイド」を参照してください。
7	PVST+ で動作させたい VLAN が，Ring Protocol の vlan-mapping に単一で設定されていることを確認してください。	対象 VLAN を Ring Protocol の vlan-mapping に設定していない場合は設定してください。また，vlan-mapping に VLAN を複数設定している場合は，vlan-mapping の構成を見直して単一 VLAN だけを設定してください。
8	MST インスタンスで動作させたい VLAN が，Ring Protocol の vlan-mapping と一致していることを確認してください。	対象 VLAN を Ring Protocol の vlan-mapping に設定していない場合は，マルチプルスパニングツリーで動作する VLAN と一致するように設定してください。

3.6.3 Ring Protocol 機能使用時の障害

この項では，Autonomous Extensible Ring Protocol の障害について説明します。

Autonomous Extensible Ring Protocol は，リングトポロジーでのレイヤ 2 ネットワークの冗長化プロトコルで，以降，Ring Protocol と呼びます。

Ring Protocol 運用時に通信ができない場合は，解析フローに従って，現象を把握し原因の切り分けを行ってください。

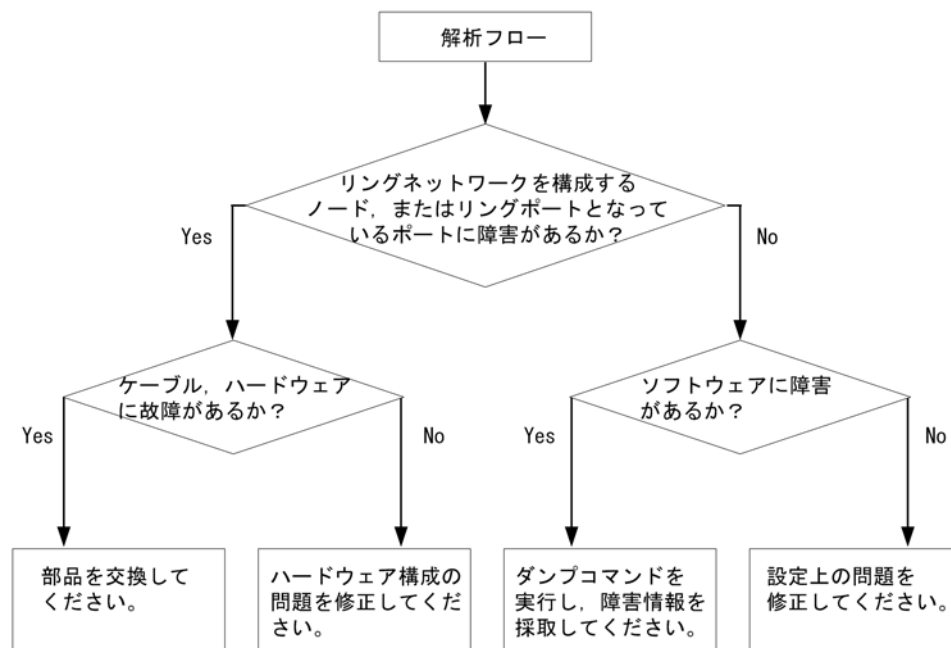
図 3-3　解析フロー

Ring Protocol 運用時に正常に動作しない場合，またはリングネットワークの障害を検出する場合は，該当のリングネットワークを構成するすべてのノードに対して，次の表に示す障害解析方法に従って，原因の切り分けを行ってください。

表 3-15　Ring Protocol の障害解析方法

項番	確認内容・コマンド	対応
1	show axrp コマンドを実行し，Ring Protocol の動作状態を確認してください。	"Oper State" の内容に "enable" が表示されている場合，項番 3 へ。
		"Oper State" の内容に "-" が表示されている場合，Ring Protocol が動作するために必要なコンフィグレーションに設定されていないものがあります。コンフィグレーションを確認してください。
		"Oper State" の内容に "disable" が表示されている場合，Ring Protocol は無効となっています。コンフィグレーションを確認してください。
		"Oper State" の内容に "Not Operating" が表示されている場合，Ring Protocol が動作していません。コンフィグレーションに矛盾（本装置の動作モード，および属性とリングポートの組み合わせが適切でないなど）がないか，コンフィグレーションを確認してください。コンフィグレーションに矛盾がない場合，項番 3 へ。
2	show logging コマンドを実行し，Ring Protocol の初期動作として MAC アドレステーブルへのエントリ登録の正常性を確認してください。	"The MAC address entry can't be registered at hardware tables." のメッセージが出力されていない場合には，項番 3 へ。
		"The MAC address entry can't be registered at hardware tables." のメッセージが出力されている場合には，Ring Protocol が動作する上で必要な MAC アドレステーブルへのエントリ設定に失敗しています。マニュアル「メッセージ・ログレファレンス」の該当個所を参照し，［対応］の記述内容に従って対応してください。
3	show axrp コマンドを実行し，動作モードと属性を確認してください。	"Mode" と "Attribute" の内容がネットワーク構成どおりの動作モードと属性になっている場合には，項番 4 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。

項番	確認内容・コマンド	対応
4	show axrp コマンドを実行し，各 VLAN グループのリングポート，およびその状態を確認してください。	"Ring Port" と "Role/State" の内容がネットワーク構成どおりのポートと状態になっている場合には，項番 5 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。
5	show axrp detail コマンドを実行し，制御 VLAN ID を確認してください。	"Control VLAN ID" の内容がネットワーク構成どおりの VLAN ID となっている場合は，項番 6 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。 例：リングを構成する各装置で制御 VLAN ID が異なっている。
6	show axrp detail コマンドを実行し，VLAN グループに属している VLAN ID を確認してください。	"VLAN ID" の内容がネットワーク構成どおりの VLAN ID となっている場合は，項番 7 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。 例：リングを構成する各装置で VLAN グループに属している VLAN ID が異なっている。
7	show axrp detail コマンドを実行し，ヘルスチェックフレームの送信間隔のタイマ値とヘルスチェックフレームの保護時間のタイマ値を確認してください。	ヘルスチェックフレームの保護時間のタイマ値 "Health Check Hold Time" が，ヘルスチェックフレームの送信間隔のタイマ値 "Health Check Interval" より大きい（伝送遅延も考慮されている）場合は，項番 8 へ。
		ヘルスチェックフレームの保護時間のタイマ値がヘルスチェックフレームの送信間隔のタイマ値より小さい，または等しい（伝送遅延が考慮されていない）場合には，コンフィグレーションを確認し，設定を見直してください。
8	show vlan detail コマンドを実行し，Ring Protocol で使用している VLAN とそのポートの状態を確認してください。	VLAN およびそのポートの状態に異常がない場合は，項番 9 へ。 また，スパニングツリーまたは GSRP を併用する構成の場合には項番 10 も，多重障害監視機能を適用する構成の場合には項番 11 も確認してください。
		異常がある場合は，コンフィグレーションの確認も含め，その状態を復旧してください。
9	フィルタ，QoS 制御の設定を確認してください。	フィルタ，QoS 制御によって，Ring Protocol で使用する制御フレームが廃棄されている可能性があります。「3.22.1　フィルタ /QoS 設定情報の確認」を参照し，確認してください。また，マニュアル「コンフィグレーションガイド」を参照してください。
10	スパニングツリー，または GSRP を併用する構成の場合，仮想リンクの設定を確認してください。	仮想リンクの設定がネットワーク構成どおりの設定となっているか，コンフィグレーションを確認してください。 • Ring Protocol とスパニングツリー，または GSRP を併用している装置で，仮想リンクの設定がされているか確認してください。 • リングネットワーク全体の装置で，仮想リンクに使用している VLAN が Ring Protocol の VLAN グループに設定されているか確認してください。
11	多重障害監視機能を適用している場合は，show axrp detail コマンドを実行し，多重障害監視の監視モードを確認してください。	共有ノードに "monitor-enable"，その他の装置に "transport-only" が設定されている場合は，項番 12 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。
12	show axrp detail コマンドを実行し，バックアップリング ID と多重障害監視用 VLAN ID を確認してください。	"Backup Ring ID" と "Control VLAN ID" がネットワーク構成どおりのバックアップリング ID と多重障害監視用 VLAN ID になっている場合は，項番 13 へ。
		上記が異なる場合には，コンフィグレーションを確認してください。
13	show axrp detail コマンドを実行し，多重障害監視フレーム送信間隔のタイマ値，および多重障害監視フレームを受信しないで多重障害発生と判断するまでの保護時間のタイマ値を確認してください。	"Multi Fault Detection Hold Time" が，"Multi Fault Detection Interval" より大きい（伝送遅延も考慮されている）ことを確認してください。
		上記が異なる場合には，コンフィグレーションを確認してください。

3.6.4 IGMP snooping によるマルチキャスト中継ができない

IGMP snooping 使用時にマルチキャスト中継ができない場合は，解析フローに従い，次の表に示す対応で現象を把握し，原因の切り分けを行ってください。

図 3-4 解析フロー

表 3-16　マルチキャスト中継の障害解析方法

項番	確認内容・コマンド	対応
1	show logging コマンドで障害発生の有無を確認してください。	以下の内容を確認してください。 • 物理的な障害のログ情報があるかを確認してください。
2	フィルタおよび QoS 制御の設定が正しいか確認してください。	フィルタによって特定のパケットが廃棄されている，または QoS 制御の帯域監視，廃棄制御もしくはシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築での帯域監視，廃棄制御またはシェーパのシステム運用が適切であるかを確認してください。 手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

3	IPv4 マルチキャストを同時使用する場合の設定が正しいか確認してください。	以下の内容を確認してください。
		• コンフィグレーションコマンド swrt_multicast_table の設定が反映されているか確認してください。
		
		コンフィグレーションコマンド swrt_multicast_table が正しく設定されている場合，show system コマンドで表示される「Current selected swrt_multicast_table:」の項目内容に On が表示されます。
		
		`Current selected swrt_multicast_table: On`
		
		コンフィグレーションコマンド swrt_multicast_table を設定しているのに項目内容が Off の場合は，装置再起動が必要です。
		
		• IPv4 マルチキャストと IGMP snooping を同時に使用する場合，該当 VLAN に IPv4 マルチキャストを必ず使用してください。
		
		該当 VLAN に IPv4 マルチキャストを使用している場合，show igmp-snooping コマンドで表示される「IPv4 Multicast routing:」の項目内容に On が表示されます。
		
		`IPv4 Multicast routing: On`
		
		• 該当 VLAN に IPv4 マルチキャストの静的グループ参加機能を使用している場合，マルチキャスト通信が必要なポートにマルチキャストルータポートを設定してください。
		
		• IGMP snooping の登録エントリ数が収容条件を超えた場合，超過後に生成した IPv4 マルチキャストのマルチキャスト中継エントリはマルチキャストルータポートだけの通信となります。IGMP snooping の登録エントリ数を超えないようにネットワークを構成してください。
		
		IGMP snooping の登録エントリ数が収容条件を超えた場合，以下のログ情報が表示されます。
		
		`IGMP snooping: The number of the IGMP snooping entry exceeded the capacity of this system.`

項番	確認内容・コマンド	対応

4	IGMP snooping の構成を show igmp-snooping コマンドで確認してください。	以下の内容を確認してください。
		• グループメンバを監視する IGMP クエリアの存在を確認するため，以下に示すメッセージが表示されていることを確認してください。
		
		(1) IGMP クエリアが存在する場合，IGMP クエリアの IP アドレスが表示されます。
		`IGMP querying system: 192.168.11.20*`
		
		(2) IGMP クエリアが存在しない場合は，「IGMP querying system:」の項目内容に何も表示されません。
		`IGMP querying system:`
		
		• 本装置が IGMP クエリアの場合，VLAN に IP アドレスが設定されていることを確認してください。
		
		(1) VLAN に IP アドレスが設定されている場合，メッセージが表示されます。
		`IP Address: 192.168.11.20*`
		
		(2) VLAN に IP アドレスが設定されていない場合，「IP Address:」の項目内容に何も表示されません。
		`IP Address:`
		
		• マルチキャストルータを接続している場合，mrouter-port を確認してください。
		
		`> show igmp-snooping 100`
		`Date 20XX/12/15 15:20:00`
		`VLAN 100:`
		`  IP Address:192.168.11.20   Querier : enable`
		`  IGMP querying system : 192.168.11.20`
		`  Port (2): 1/1,1/3`
		`  Mrouter-port:1/1`
		`  Group Counts: 3`

5	show igmp-snooping コマンドで group パラメータを指定し IPv4 マルチキャストグループアドレスを確認してください。	以下の内容を確認してください。
		• 加入した IPv4 マルチキャストグループアドレスが show igmp-snooping group で表示されていることを確認してください。
		
		`> show igmp-snooping group 100`
		`Date 20XX/12/15 15:20:00`
		`  VLAN 100  Group counts:3`
		`   Group Address     MAC Address`
		`    224.10.10.10   0100.5e0a.0a0a`
		`      Port-list  1/1-3`
		`    225.10.10.10   0100.5e0a.0a0a`
		`      Port-list  1/1-2`
		`    239.192.1.1    0100.5e40.1606`
		`      Port-list  1/1`

注※　本装置が IGMP クエリアの場合は，IGMP querying system で表示されているアドレスと IP Address で表示されているアドレスは一致するが，他装置が IGMP クエリアの場合は，IGMP querying system で表示されているアドレスと IP Address で表示されているアドレスは一致しません。

3.6.5　MLD snooping によるマルチキャスト中継ができない

MLD snooping 使用時にマルチキャスト中継ができない場合は，解析フローに従い，次の表に示す対応で現象を把握し，原因の切り分けを行ってください。

図 3-5　解析フロー

表 3-17　マルチキャスト中継の障害解析方法

項番	確認内容・コマンド	対応
1	show logging コマンドで障害発生の有無を確認してください。	以下の内容を確認してください。 • 物理的な障害のログ情報があるかを確認してください。

<table>
<tr><th>項番</th><th>確認内容・コマンド</th><th>対応</th></tr>
<tr><td>2</td><td>フィルタおよび QoS 制御の設定が正しいか確認してください。</td><td>フィルタによって特定のパケットが廃棄されている，または QoS 制御の帯域監視，廃棄制御もしくはシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築での帯域監視，廃棄制御またはシェーパのシステム運用が適切であるかを確認してください。手順については，「3.22.1 フィルタ /QoS 設定情報の確認」を参照してください。</td></tr>
<tr><td>3</td><td>IPv6 マルチキャストを同時使用する場合の設定が正しいか確認してください。</td><td>以下の内容を確認してください。
• コンフィグレーションコマンド swrt_multicast_table の設定が反映されているか確認してください。

コンフィグレーションコマンド swrt_multicast_table が正しく設定されている場合，show system コマンドで表示される「Current selected swrt_multicast_table:」の項目内容に On が表示されます。

<code>Current selected swrt_multicast_table: On</code>

コンフィグレーションコマンド swrt_multicast_table を設定しているのに項目内容が Off の場合は，装置再起動が必要です。

• IPv6 マルチキャストと MLD snooping を同時に使用する場合，該当 VLAN に IPv6 マルチキャストを必ず使用してください。

該当 VLAN に IPv6 マルチキャストを使用している場合，show mld-snooping コマンドで表示される「IPv6 Multicast routing:」の項目内容に On が表示されます。

<code>IPv6 Multicast routing: On</code>

• 該当 VLAN に IPv6 マルチキャストの静的グループ参加機能を使用している場合，マルチキャスト通信が必要なポートにマルチキャストルータポートを設定してください。

• MLD snooping の登録エントリ数が収容条件を超えた場合，超過後に生成した IPv6 マルチキャストのマルチキャスト中継エントリはマルチキャストルータポートだけの通信となります。MLD snooping の登録エントリ数を超えないようにネットワークを構成してください。

MLD snooping の登録エントリ数が収容条件を超えた場合，以下のログ情報が表示されます。

<code>MLD snooping: The number of the MLD snooping entry exceeded the capacity of this system.</code></td></tr>
</table>

<table>
<tr><th>項番</th><th>確認内容・コマンド</th><th>対応</th></tr>
<tr><td>4</td><td>MLD snooping の構成を show mld-snooping コマンドで確認してください。</td><td>以下の内容を確認してください。
• グループメンバを監視する MLD クエリアの存在を確認するため，以下に示すメッセージが表示されていることを確認してください。

(1) MLD クエリアが存在する場合，MLD クエリアの IP アドレスが表示されます。
MLD querying system: fe80::200:87ff:fe10:1959*

(2) MLD クエリアが存在しない場合は，「MLD querying system:」の項目内容に何も表示されません。
MLD querying system:

• 本装置が MLD クエリアの場合，VLAN に IP アドレスが設定されていることを確認してください。

(1) VLAN に IP アドレスが設定されている場合，以下のメッセージが表示されます。
IP Address: fe80::200:87ff:fe10:1959*

(2) VLAN に IP アドレスが設定されていない場合，「IP Address:」の項目内容に何も表示されません。
IP Address:

• マルチキャストルータを接続している場合，mrouter-port を確認してください。

>show mld-snooping 100
Date 20XX/12/15 15:20:00
VLAN 100:
IP Address:fe80::200:87ff:fe10:1959 Querier : enable
  MLD querying system: fe80::200:87ff:fe10:1959
  Port(2): 1/1,1/3
  Mrouter-port: 1/1
  Group Count :3</td></tr>
<tr><td>5</td><td>show mld-snooping コマンドで group パラメータを指定し IPv6 マルチキャストグループアドレスを確認してください。</td><td>以下の内容を確認してください。
• 加入した IPv6 マルチキャストグループアドレスが show mld-snooping group で表示されていることを確認してください。

> show mld-snooping group 100
Date 20XX/12/15 15:20:00
VLAN 100 Group count:2
 Group Address   MAC Address
  ff0e::0e0a:0a01 3333.0e0a.0a01
      Port-list 1/1-3
  ff0e::0102:0c11 3333.0102.0c11
      Port-list 1/1-2</td></tr>
</table>

注※　本装置が MLD クエリアの場合は，MLD querying system で表示されているアドレスと IP Address で表示されているアドレスは一致するが，他装置が MLD クエリアの場合は，MLD querying system で表示されているアドレスと IP Address で表示されているアドレスは一致しません。

3.7 IPv4 ネットワークの通信障害

3.7.1 通信できない，または切断されている

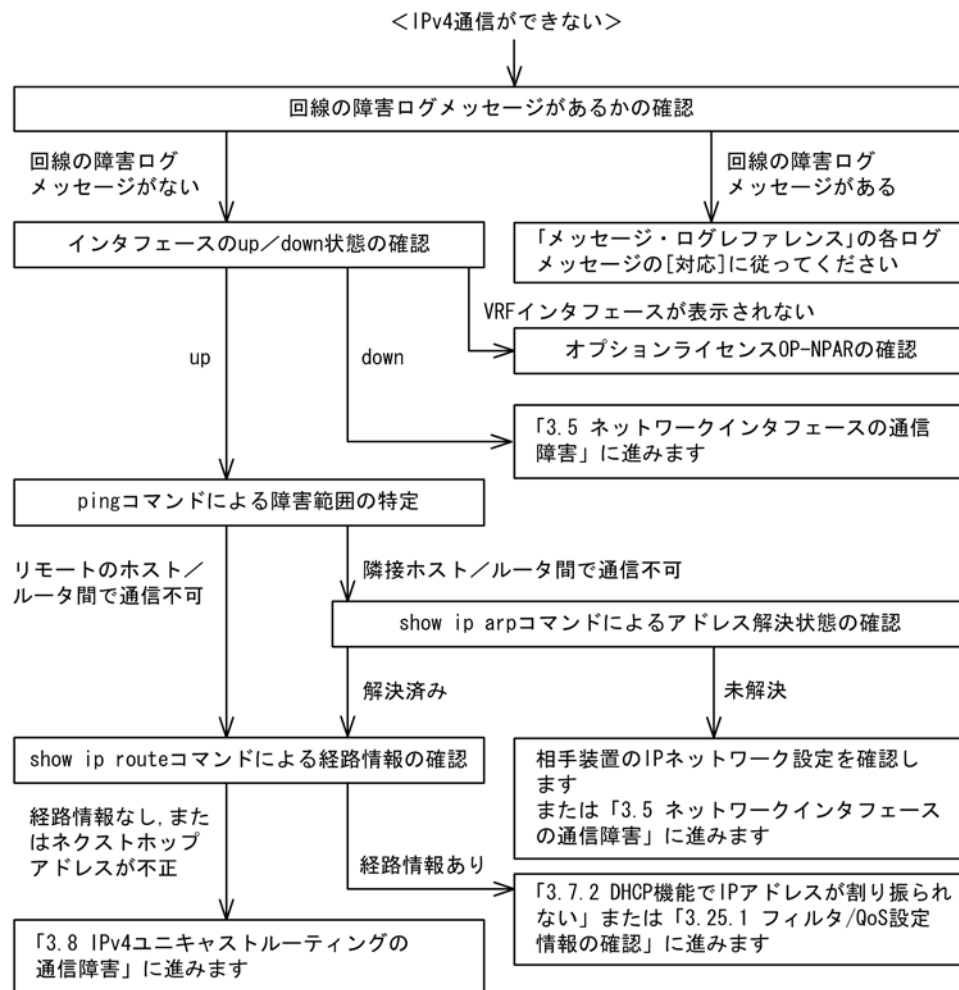
本装置を使用している IPv4 ネットワーク上で，通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. IP 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

上記 1. および 2. については，コンフィグレーションおよびネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

ここでは，3. に示すように「コンフィグレーションおよびネットワーク構成は正しいのに IP 通信ができない」，「これまで正常に動いていたのに IP 通信ができなくなった」というケースを中心に，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローに従ってください。

図 3-6 IPv4 通信ができない場合の障害解析手順

(1) ログの確認

通信ができなくなる原因の一つには，回線の障害（または壊れ）が考えられます。本装置が表示するログで，ハードウェアの障害を示すメッセージの表示手順を示します。

なお，ログの内容については，マニュアル「メッセージ・ログレファレンス」を参照してください。

1. 本装置にログインします。
2. show logging コマンドを使ってログを表示させます。
3. ログには各々発生した日時が表示されます。通信ができなくなった日時にログが表示されていないか確認してください。
4. 通信ができなくなった日時に表示されているログの障害の内容および障害への対応については，マニュアル「メッセージ・ログレファレンス」に記載しています。その指示に従ってください。
5. 通信ができなくなった日時にログの表示がないときは，「(2) インタフェース状態の確認」に進んでください。

(2) インタフェース状態の確認

本装置のハードウェアは正常に動作している場合でも，本装置と接続している隣接の装置のハードウェアに障害が発生していることも考えられます。

本装置と隣接の装置間の，インタフェースの状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip interface コマンドを使って該当装置間のインタフェースの Up ／ Down 状態を確認してください。
3. 該当インタフェースが”Down”状態のときは，「3.5　ネットワークインタフェースの通信障害」を参照してください。
4. 該当インタフェースとの間のインタフェースが”Up”状態のときは，「(3) 障害範囲の特定（本装置から実施する場合)」に進んでください。

(3) 障害範囲の特定（本装置から実施する場合）

本装置に障害がない場合は，通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか，障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping コマンドを使って通信できない両方の相手との疎通を確認してください。ping コマンドの操作例および実行結果の見方は，マニュアル「コンフィグレーションガイド」を参照してください。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping コマンド実行の結果，障害範囲が隣接装置の場合は「(5) 隣接装置との ARP 解決情報の確認」に，リモート先の装置の場合は「(6) ユニキャストルーティング情報の確認」に進んでください。

(4) 障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインできない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping 機能があることを確認してください。
2. ping 機能をお使いになり，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping 機能で通信相手との疎通が確認できなかったときは，さらに ping コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping 機能による障害範囲が特定できましたら，障害と考えられる装置が本装置である場合は本装置に

ログインしていただき，障害解析フローに従って障害原因の調査を行ってください。

(5) 隣接装置との ARP 解決情報の確認

ping コマンドの実行結果によって隣接装置との疎通が不可の場合は，ARP によるアドレスが解決していないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip arp コマンドを使って隣接装置間とのアドレス解決状態（ARP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（ARP エントリ情報あり）場合は，「(6) ユニキャストルーティング情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（ARP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が一致しているかを確認してください。
5. DHCP snooping を使用している場合はダイナミック ARP 検査によってパケットが廃棄されている可能性があります。コンフィグレーションの DHCP snooping の設定条件が正しいか見直してください。手順については，「3.23　DHCP snooping のトラブル」を参照してください。

(6) ユニキャストルーティング情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない場合や，IPv4 ユニキャスト通信で通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを実行して，本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「3.8　IPv4 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - DHCP ／ BOOTP 機能
     「(7) DHCP/BOOTP 設定情報の確認」に進んでください。
   - フィルタ／ QoS 機能
     「(8) フィルタ /QoS 設定情報の確認」に進んでください。

(7) DHCP/BOOTP 設定情報の確認

本装置の DHCP ／ BOOTP のリレーまたはサーバ機能によって隣接装置へ IP アドレスを割り振っている場合は，適切に IP アドレスを割り振れていない可能性があります。

コンフィグレーションの DHCP ／ BOOTP のリレーまたはサーバ機能の設定条件が正しいか見直してください。手順については，「3.7.2　DHCP 機能で IP アドレスが割り振られない」を参照してください。

(8) フィルタ /QoS 設定情報の確認

フィルタによって特定のパケットが廃棄されているか，QoS 制御の帯域監視，廃棄制御もしくはシェーパによってパケットが廃棄されている可能性があります。

コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築での帯域監視，廃棄制御またはシェーパのシステム運用が適切であるか見直してください。手順については，「3.22.1　フィ

ルタ /QoS 設定情報の確認」を参照してください。

また，DHCP snooping を使用している場合は端末フィルタによってパケットが廃棄されている可能性があります。コンフィグレーションの DHCP snooping の設定条件が正しいか見直してください。手順については，「3.23　DHCP snooping のトラブル」を参照してください。

3.7.2　DHCP 機能で IP アドレスが割り振られない

(1) DHCP/BOOTP リレーの通信トラブル

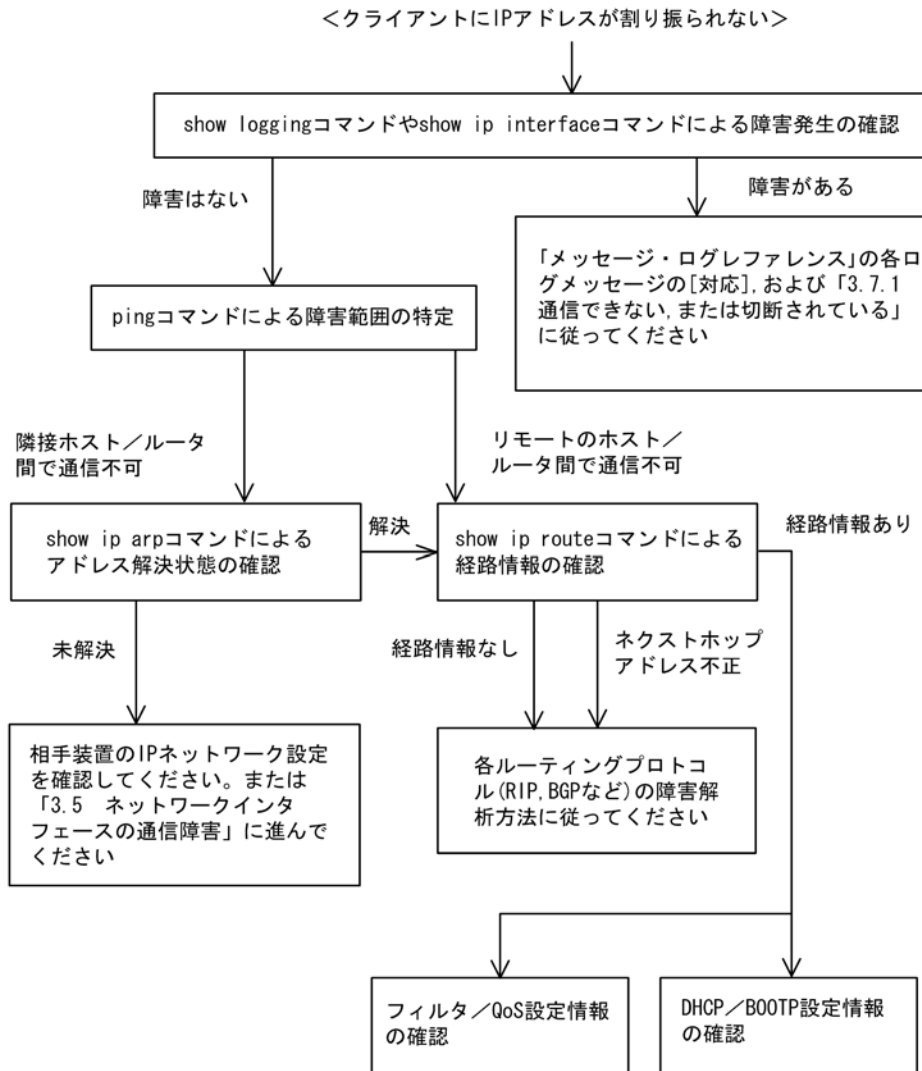
DHCP ／ BOOTP リレーの通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. DHCP ／ BOOTP リレー通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. DHCP ／ BOOTP サーバの障害

上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

ここでは，クライアントの設定（ネットワークカードの設定，ケーブルの接続など）は確認されているものとし，上記 1. および 3. に示すような「コンフィグレーションの変更を行ったら，DHCP ／ BOOTP サーバから IP アドレスが割り振られなくなった」，「コンフィグレーションおよびネットワーク構成は正しいのにクライアントに IP アドレスが割り振られず，IP 通信できない」，というケースについて，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローに従ってください。

図 3-7　DHCP/BOOTP リレーの障害解析手順

(a)　ログおよびインタフェースの確認

クライアントに IP アドレスが割り振られなくなる原因の一つにクライアントーサーバ間で通信ができなくなっていることが考えられます。本装置が表示するログや show ip interface コマンドによるインタフェースの up ／ down 状態を確認してください。手順については「3.7.1　通信できない，または切断されている」を参照してください。

(b)　障害範囲の特定（本装置から実施する場合）

本装置に障害がないときは通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping コマンドを使って通信できない両方の相手との疎通を確認してください。ping コマンドの操作例および実行結果の見方は，マニュアル「コンフィグレーションガイド」を参照してください。
3. ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping コマンド実行の結果，障害範囲が隣接装置の場合は「(d)　隣接装置との ARP 解決情報の確認」に，リモート先の装置の場合は「(e)　経路情報の確認」に進んでください。

(c) 障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインできない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping 機能があることを確認してください。
2. ping 機能をお使いになり，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping 機能で通信相手との疎通が確認できなかったときは，さらに ping コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping 機能による障害範囲の特定ができましたら，障害と考えられる装置が本装置である場合は本装置にログインしていただき，障害解析フローに従って障害原因の調査を行ってください。

(d) 隣接装置との ARP 解決情報の確認

ping コマンドによって隣接装置との疎通が不可のときは，ARP によるアドレスが解決していないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ip arp コマンドを使って隣接装置間とのアドレス解決状態（ARP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（ARP エントリ情報あり）場合は，「(e) 経路情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（ARP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が疎通できる設定になっているかを確認してください。
5. DHCP snooping を使用している場合はダイナミック ARP 検査によってパケットが廃棄されている可能性があります。コンフィグレーションの DHCP snooping の設定条件が正しいか見直してください。手順については，「3.23　DHCP snooping のトラブル」を参照してください。

(e) 経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない，通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを使って本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「3.8　IPv4 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
    - フィルタ／ QoS 機能
      「(f) フィルタ /QoS 設定情報の確認」に進んでください。
    - DHCP ／ BOOTP 機能
      「(g) DHCP/BOOTP 設定情報の確認」に進んでください。

(f) フィルタ /QoS 設定情報の確認

フィルタによって特定のパケットだけを廃棄する設定になっているか，QoS 制御の帯域監視，廃棄制御またはシェーパによってパケットが廃棄されている可能性があります。

コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築での帯域監視，廃

棄制御またはシェーパのシステム運用が適切であるかを確認してください。手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

また，DHCP snooping を使用している場合は端末フィルタによってパケットが廃棄されている可能性があります。コンフィグレーションの DHCP snooping の設定条件が正しいか見直してください。手順については，「3.23　DHCP snooping のトラブル」を参照してください。

(g) DHCP/BOOTP 設定情報の確認

DHCP ／ BOOTP サーバに貸し出し用 IP アドレスが十分に残っている場合，DHCP ／ BOOTP リレーのコンフィグレーション設定ミスによってクライアントに IP アドレスが割り振られないという原因が考えられます。次にコンフィグレーションの確認手順を示します。

1. ip helper-address は DHCP ／ BOOTP サーバの IP アドレス，または DHCP ／ BOOTP リレーエージェント機能付き次ルータの IP アドレスが指定されているか確認してください。
2. クライアント側のインタフェースに ip helper-address が設定されているか確認してください。
3. ip bootp-hops の値がクライアントから見て正しい bootp hops 値となっているか確認してください。
4. マルチホーム構成の場合は ip relay-agent-address の値と DHCP/BOOTP サーバで配布する IP アドレスのサブネットが一致しているか確認してください。
5. DHCP snooping を使用している場合は DHCP snooping によってパケットが廃棄されている可能性があります。コンフィグレーションの DHCP snooping の設定条件が正しいか見直してください。手順については，「3.23　DHCP snooping のトラブル」を参照してください。

(h) DHCP リレーと VRRP が同一インタフェースで運用されている場合の確認

DHCP ／ BOOTP リレーと VRRP が同一インタフェースで運用されている場合，DHCP ／ BOOTP サーバで，DHCP ／ BOOTP クライアントゲートウェイアドレス（ルータオプション）を VRRP コンフィグレーションで設定した仮想ルータアドレスに設定しなければなりません。設定しなかった場合，VRRP によるマスタ・スタンバイルータ切り替え後，DHCP ／ BOOTP クライアントが通信できなくなる可能性があります。確認方法については各 DHCP ／ BOOTP サーバの確認方法に従ってください。

(2) DHCP サーバの通信トラブル

DHCP サーバの通信トラブル（クライアントにアドレス配信できない）が発生する要因として考えられるのは，次の 3 種類があります。

1. コンフィグレーションの設定ミス
2. ネットワークの構成変更
3. DHCP サーバの障害

まず上記 1. の確認を行ってください。コンフィグレーションの設定で間違えやすいものを例にとり説明します。上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。クライアント／サーバの設定（ネットワークカードの設定，ケーブルの接続など）は確認されている場合，上記 3. に示すような「コンフィグレーションおよびネットワーク構成は正しいのにクライアントに IP アドレスが割り振られず，IP 通信できない」，というケースについては，詳細を「(b) ログメッセージおよびインタフェースの確認」〜「(e) フィルタ /QoS 設定情報の確認」に示します。

障害部位および原因の切り分け手順を次のフローに示します。

図 3-8　DHCP サーバの障害解析手順

<クライアントにIPアドレスが割り振られない>

コンフィグレーションの確認

show loggingコマンドやshow ip interface
コマンドによる障害発生の確認

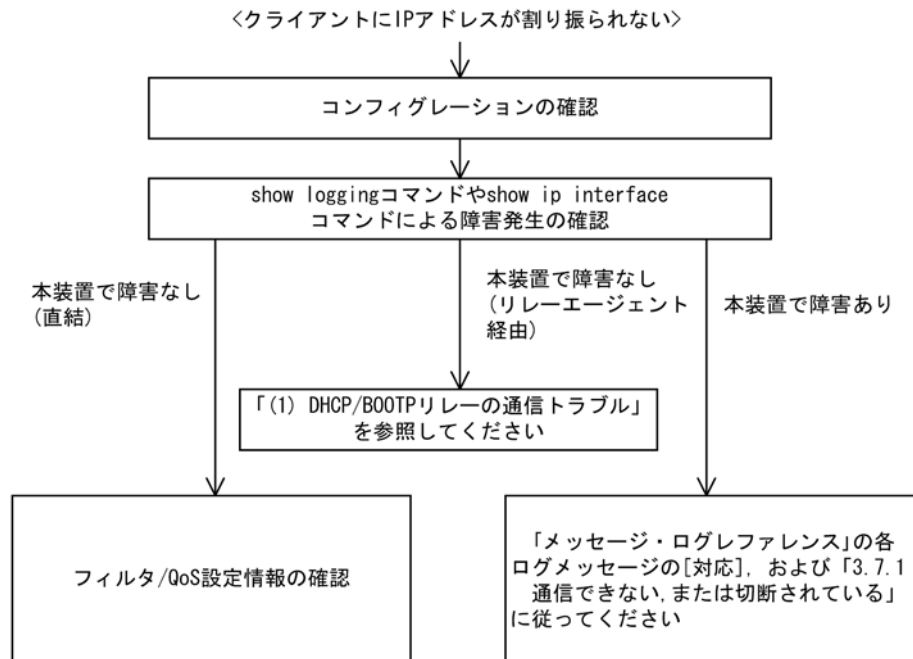
本装置で障害なし
（直結）

本装置で障害なし
（リレーエージェント
経由）

本装置で障害あり

「(1) DHCP/BOOTPリレーの通信トラブル」
を参照してください

フィルタ/QoS設定情報の確認

「メッセージ・ログレファレンス」の各
ログメッセージの[対応]，および「3.7.1
通信できない，または切断されている」
に従ってください

(a) コンフィグレーションの確認

DHCP サーバ上のリソース類のコンフィグレーション設定ミスによってクライアントに IP アドレスが割り振られないという原因が考えられます。コンフィグレーションの確認手順を次に示します。

1. DHCP クライアントに割り付ける IP アドレスの network 設定を含む ip dhcp pool 設定が存在することを，コンフィグレーションで確認してください。
2. DHCP クライアントに割り付ける DHCP アドレスプール数がコンフィグレーションコマンド ip dhcp excluded-address によって同時使用するクライアントの台数分以下になっていないかを，コンフィグレーションで確認してください。
3. クライアントが本装置からアドレスを割り振られたあと，クライアントと他装置との通信ができない場合は，デフォルトルータの設定がされていないことがあります。コンフィグレーションコマンド default-router でクライアントが接続されているネットワークのルータアドレス（デフォルトルータ）が設定されているか確認してください（マニュアル「コンフィグレーションコマンドレファレンス」を参考にしてください）。
4. DHCP リレーエージェントとなる装置の設定を確認してください。リレーエージェントも本装置を使用している場合，「(1) DHCP/BOOTP リレーの通信トラブル」を参照してください。
5. DHCP snooping を使用している場合は DHCP snooping によってパケットが廃棄されている可能性があります。コンフィグレーションの DHCP snooping の設定条件が正しいか見直してください。手順については，「3.23　DHCP snooping のトラブル」を参照してください。

(b) ログメッセージおよびインタフェースの確認

クライアントに IP アドレスが割り振られなくなる原因の一つにクライアントーサーバ間で通信ができなくなっていることが考えられます。本装置が表示するログメッセージや show ip interface コマンドによるインタフェースの up ／ down 状態を確認してください。手順については「3.7.1　通信できない，または切断されている」を参照してください。

(c) 障害範囲の特定（本装置から実施する場合）

本装置に障害がないときは通信を行っていた相手との間のどこかに障害が発生している可能性があります。

通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. クライアントとサーバ間にルータなどがある場合，ping コマンドを使って通信できない相手（DHCP クライアント）との間にある装置（ルータ）の疎通を確認してください。ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置からクライアント側に向けて近い装置から順に通信相手に向けて疎通を確認してください。ping コマンドの操作例および実行結果の見方については，マニュアル「コンフィグレーションガイド」を参照してください。
3. サーバとクライアントが直結の場合，HUB やケーブルの接続を確認してください。
4. ping コマンドによる障害範囲が隣接装置かリモートの装置かによって，障害解析フローの次のステップに進んでください。

(d) 経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない，通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを使って本装置が取得した経路情報を確認してください。

(e) フィルタ /QoS 設定情報の確認

フィルタによって特定のパケットだけが廃棄されているか，QoS 制御の帯域監視，廃棄制御またはシェーパによってパケットが廃棄されている可能性があります。

コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築での帯域監視，廃棄制御またはシェーパのシステム運用が適切であるか，本装置およびクライアント・サーバ間にある中継装置で見直しを行ってください。手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

また，DHCP snooping を使用している場合は端末フィルタによってパケットが廃棄されている可能性があります。コンフィグレーションの DHCP snooping の設定条件が正しいか見直してください。手順については，「3.23　DHCP snooping のトラブル」を参照してください。

(f) レイヤ 2 ネットワークの確認

(a) から (e) までの手順で設定ミスや障害が見つからない場合は，レイヤ 2 ネットワークに問題がある可能性があります。「3.6　レイヤ 2 ネットワークの通信障害」を参考にレイヤ 2 ネットワークの確認を行ってください。

3.7.3　DHCP 機能で DynamicDNS 連携が動作しない

(1) DHCP サーバの通信トラブル

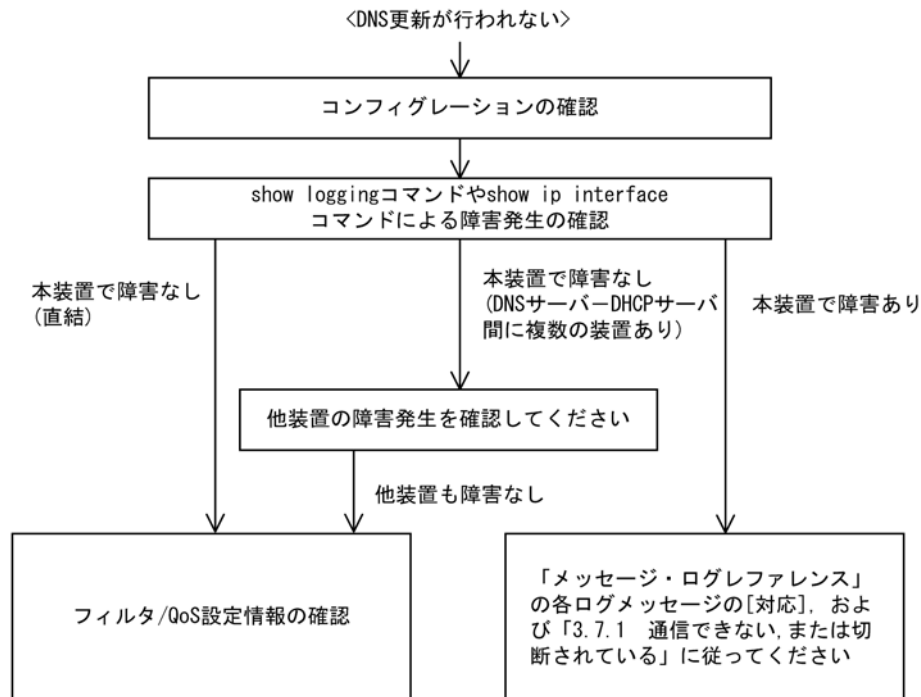
DHCP サーバの通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. コンフィグレーションの設定ミス
2. ネットワークの構成変更
3. DHCP サーバの障害

まず上記 1. の確認を行ってください。コンフィグレーションの設定で間違えやすいものを例にとり説明します。上記 2. については，ネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。DNS サーバ／ DHCP サーバの設定（ネットワークカードの

設定，ケーブルの接続など）は確認されている場合，上記 3. に示すような「コンフィグレーションおよびネットワーク構成は正しいのに DynamicDNS 連携が動作しない」，というケースについては，詳細を「(b) 時刻情報の確認」～「(f) フィルタ /QoS 設定情報の確認」に示します。

障害部位および原因の切り分け手順を次のフローに示します。

図 3-9　DNS 連携時の DHCP サーバ障害解析手順

(a) コンフィグレーションの確認

DHCP サーバ上のミス，または DNS サーバ上の設定との不一致によって DynamicDNS に対する DNS 更新が正しく動作していないことが原因と考えられます。コンフィグレーションの確認手順を次に示します。

1. 始めに DNS サーバ側で DNS 更新を許可する方法を確認してください。IP アドレス／ネットワークによるアクセス許可の場合は項目 3 以降を参照してください。認証キーによる許可の場合は項目 2 以降を参照してください。
2. DNS サーバ側で指定しているキー情報，認証キーと DHCP サーバコンフィグレーションで設定されているキー情報が同じであることを確認してください（マニュアル「コンフィグレーションコマンドレファレンス」を参考にしてください)。
3. DNS サーバ側で指定しているゾーン情報と DHCP サーバコンフィグレーションのゾーン情報が一致していることを確認してください（マニュアル「コンフィグレーションコマンドレファレンス」を参考にしてください)。また，このときに正引きと逆引きの両方が設定されていることを確認してください。
4. DNS 更新が設定されていることを確認してください（マニュアル「コンフィグレーションコマンドレファレンス」を参考にしてください)。デフォルトでは DNS 更新は無効になっているため，DNS 更新を行う場合は本設定を行う必要があります
5. クライアントが使用するドメイン名が DNS サーバに登録してあるドメイン名と一致していることを確認してください。DHCP によってドメイン名を配布する場合はコンフィグレーションで正しく設定されていることを確認してください（マニュアル「コンフィグレーションコマンドレファレンス」およびマニュアル「運用コマンドレファレンス」を参考にしてください)。

(b) 時刻情報の確認

DNS 更新で認証キーを使用するとき，本装置と DNS サーバが指す時刻の差は多くの場合 UTC 時間で 5 分以内である必要があります。show clock コマンドで本装置の時刻情報を確認して，必要ならばマニュアル「コンフィグレーションコマンドレファレンス」を参考に時刻情報の同期を行ってください。

(c) ログメッセージおよびインタフェースの確認

DNS サーバとの通信ができなくなる原因の一つに DNS サーバー DHCP サーバ間で通信ができなくなっていることが考えられます。本装置が表示するログメッセージや show ip interface コマンドによるインタフェースの up ／ down 状態を確認してください。手順については「3.7.1　通信できない，または切断されている」を参照してください。

(d) 障害範囲の特定（本装置から実施する場合）

本装置に障害がないときは通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. DNS サーバと DHCP サーバ間にルータなどがある場合，ping コマンドを使って通信できない相手（DNS サーバ）との間にある装置（ルータ）の疎通を確認してください。ping コマンドで通信相手との疎通が確認できなかったときは，さらに ping コマンドを使って本装置からクライアント側に向けて近い装置から順に通信相手に向けて疎通を確認してください。ping コマンドの操作例および実行結果の見方については，マニュアル「コンフィグレーションガイド」を参照してください。
3. DNS サーバと DHCP サーバが直結の場合，HUB やケーブルの接続を確認してください。
4. ping コマンドによる障害範囲が隣接装置かリモートの装置かによって，障害解析フローの次のステップに進んでください。

(e) 経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない，通信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ip route コマンドを使って本装置が取得した経路情報を確認してください。

(f) フィルタ /QoS 設定情報の確認

フィルタによって特定のパケットだけが廃棄されているか，QoS 制御の帯域監視，廃棄制御またはシェーパによってパケットが廃棄されている可能性があります。

コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築での帯域監視，廃棄制御またはシェーパのシステム運用が適切であるか，本装置および DNS サーバ・DHCP サーバ間にある中継装置でも見直しを行ってください。手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

また，DHCP snooping を使用している場合は端末フィルタによってパケットが廃棄されている可能性があります。コンフィグレーションの DHCP snooping の設定条件が正しいか見直してください。手順については，「3.23　DHCP snooping のトラブル」を参照してください。

(g) レイヤ 2 ネットワークの確認

(a) から (f) までの手順で設定ミスや障害が見つからない場合は，レイヤ 2 ネットワークに問題がある可能性があります。「3.6　レイヤ 2 ネットワークの通信障害」を参考にレイヤ 2 ネットワークの確認を行って

ください。

3.8　IPv4 ユニキャストルーティングの通信障害

3.8.1　RIP 経路情報が存在しない

本装置が取得した経路情報の表示に，RIP の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

また，ネットワーク・パーティションを使用していて，コンフィグレーションコマンド maximum routes で経路の上限値を設定している場合，まず「3.8.4　VRF で IPv4 経路情報が存在しない」の障害解析方法に従ってください。

表 3-18　RIP の障害解析方法

項番	確認内容・コマンド	対応
1	RIP の隣接情報を表示します。 show ip rip neighbor	隣接ルータのインタフェースが表示されていない場合は項番 2 へ。
		隣接ルータのインタフェースが表示されている場合は項番 3 へ。
2	コンフィグレーションで RIP 設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが RIP 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。フィルタ設定情報の確認手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

3.8.2　OSPF 経路情報が存在しない

本装置が取得した経路情報の表示に，OSPF の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

また，ネットワーク・パーティションを使用していて，コンフィグレーションコマンド maximum routes で経路の上限値を設定している場合，まず「3.8.4　VRF で IPv4 経路情報が存在しない」の障害解析方法に従ってください。

表 3-19　OSPF の障害解析方法

項番	確認内容・コマンド	対応
1	OSPF のインタフェース状態を確認します。 show ip ospf interface <IP Address>	インタフェースの状態が DR または P to P の場合は項番 3 へ。
		インタフェースの状態が BackupDR または DR Other の場合は項番 2 へ。
		インタフェースの状態が Waiting の場合は，時間を置いてコマンドを再実行してください。項番 1 へ。
2	Neighbor List より DR との隣接ルータ状態を確認します。	DR との隣接ルータ状態が Full 以外の場合は項番 4 へ。
		DR との隣接ルータ状態が Full の場合は項番 5 へ。

項番	確認内容・コマンド	対応
3	Neighbor List より全隣接ルータ状態を確認します。	一部の隣接ルータ状態が Full 以外の場合は項番 4 へ。
		全隣接ルータ状態が Full の場合は項番 5 へ。
4	コンフィグレーションで OSPF の設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 5 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
5	OSPF 経路を学習している経路を確認してください。 show ip route all-routes	経路が InActive の場合には項番 6 へ。
		経路が存在しない場合は隣接ルータが OSPF 経路を広告しているか確認してください。
6	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが OSPF 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。フィルタ設定情報の確認手順については,「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

3.8.3　BGP4 経路情報が存在しない

本装置が取得した経路情報の表示に，BGP4 の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

また，ネットワーク・パーティションを使用していて，コンフィグレーションコマンド maximum routes で経路の上限値を設定している場合，まず「3.8.4　VRF で IPv4 経路情報が存在しない」の障害解析方法に従ってください。

表 3-20　BGP4 の障害解析方法

項番	確認内容・コマンド	対応
1	BGP4 のピア状態を確認します。 show ip bgp neighbors	ピア状態が Established 以外の場合は項番 2 へ。
		ピア状態が Established の場合は項番 3 へ。
2	コンフィグレーションで BGP4 の設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	BGP4 経路を学習しているか確認してください。 show ip bgp received-routes	経路が存在するが active 状態でない場合は項番 4 へ。
		経路が存在しない場合は項番 5 へ。
4	BGP4 経路のネクストホップアドレスを解決する経路情報が存在するか確認してください。 show ip route	ネクストホップアドレスを解決する経路情報がある場合は項番 5 へ。
		ネクストホップアドレスを解決する経路情報がない場合はその経路情報を学習するためのプロトコルの障害解析を実施してください。
5	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが BGP4 経路を広告しているか確認してください。

項番	確認内容・コマンド	対応
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。フィルタ設定情報の確認手順については,「3.22.1 フィルタ /QoS 設定情報の確認」を参照してください。

3.8.4 VRF で IPv4 経路情報が存在しない

本装置が取得した経路情報の表示に，各プロトコルの経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因を切り分けてください。

表 3-21 VRF の障害解析方法

項番	確認内容・コマンド	対応
1	VRF 内の経路数がコンフィグレーションで設定した上限値以上でないか確認してください。 show ip vrf	経路数が上限値以上であれば項番 2 へ。
		経路数が上限値未満であれば，存在しない経路のプロトコルの障害解析を実施してください。 RIP :「3.8.1 RIP 経路情報が存在しない」 OSPF :「3.8.2 OSPF 経路情報が存在しない」 BGP4 :「3.8.3 BGP4 経路情報が存在しない」
2	コンフィグレーションで VRF 内の経路数の上限値を確認してください。	上限値を増やすか，経路を集約するなどして，経路数を減らしてください。

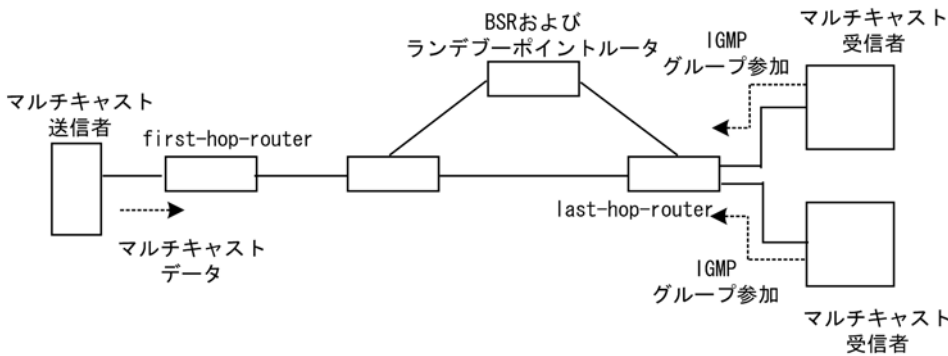
3.9　IPv4 マルチキャストルーティングの通信障害

本装置で IPv4 マルチキャスト通信障害が発生した場合の対処について説明します。

3.9.1　IPv4 PIM-SM ネットワークで通信ができない

IPv4 PIM-SM ネットワーク構成でマルチキャスト中継ができない場合は，以下に示す障害解析方法に従って原因の切り分けを行ってください。

IPv4 PIM-SM のネットワーク例を次の図に示します。

図 3-10　IPv4 PIM-SM ネットワーク例

注

- BSR：ランデブーポイントの情報を配信するルータ（詳細は，マニュアル「コンフィグレーションガイド」を参照してください）
- ランデブーポイントルータ：中継先が確定していないパケットをマルチキャスト受信者方向に中継するルータ（詳細は，マニュアル「コンフィグレーションガイド」を参照してください）
- first-hop-router：マルチキャスト送信者と直接接続するルータ
- last-hop-router：マルチキャスト受信者と直接接続するルータ

(1)　共通確認内容

次の表に，IPv4 PIM-SM ネットワーク構成のすべての本装置に対する共通確認内容を示します。

表 3-22　共通確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションにマルチキャスト機能を使用する指定（ip multicast routing）があることを確認してください。 show running-config	マルチキャスト機能を使用する指定がない場合は，コンフィグレーションを修正してください。
2	一つ以上のインタフェースで PIM-SM が動作していることを確認してください。 show ip pim interface	動作していない場合はコンフィグレーションを確認し，どれか一つ以上のインタフェースで PIM-SM が動作するように設定してください。 コンフィグレーションで PIM の動作設定をしたインタフェースが，show ip pim interface コマンドで表示されない場合は，該当インタフェースにマルチホームの設定がされていないことを確認してください。

項番	確認内容・コマンド	対応
3	PIM が動作するインタフェースに，IGMP snooping が設定されているか確認してください。 show igmp-snooping	IGMP snooping が設定されている場合は，以下の内容を確認してください。 • 隣接ルータと接続しているポートに対して IGMP snooping のマルチキャストルータポートの設定がされているか確認してください。 • 「3.6.4　IGMP snooping によるマルチキャスト中継ができない」を参照してください。
4	PIM および IGMP が動作するインタフェースで，フィルタなどによるプロトコルパケットおよびマルチキャストパケット中継を抑止する設定がないことを，コンフィグレーションで確認してください。 show running-config	プロトコルパケットおよびマルチキャストパケット中継を抑止する設定がある場合は，コンフィグレーションを修正してください。フィルタ設定情報の確認手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。
5	PIM の隣接情報を確認してください。 show ip pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM-SM が動作していることを show ip pim interface コマンドで確認してください。 • 隣接ルータの設定を確認してください。
6	マルチキャストデータ送信者へのユニキャスト経路が存在するか確認してください。 show ip route	ユニキャスト経路が存在しない場合は「3.8　IPv4 ユニキャストルーティングの通信障害」を参照してください。
7	マルチキャストデータ送信者への次ホップアドレスと接続しているインタフェースで，PIM が動作していることを確認してください。 show ip pim interface	動作していない場合はコンフィグレーションを確認し，マルチキャストデータ送信者への次ホップアドレスと接続しているインタフェースで PIM が動作するように設定してください。
8	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていないことを，コンフィグレーションで確認してください。 show running-config	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれている場合は，コンフィグレーションを修正してください。
9	BSR が決定されていることを確認してください。ただし，中継対象グループアドレスに対するランデブーポイントが静的ランデブーポイントの場合は，確認不要です。 show ip pim bsr	BSR が決定されていない場合は BSR へのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「3.8　IPv4 ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，BSR の設定を確認してください。BSR が本装置の場合は，「(2) BSR 確認内容」を参照してください。
10	ランデブーポイントが決定されていることを確認してください。 show ip pim rp-mapping	ランデブーポイントが決定されていない場合は，ランデブーポイントへのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「3.8　IPv4 ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，ランデブーポイントの設定を確認してください。ランデブーポイントが本装置の場合は，「(3) ランデブーポイントルータ確認内容」を参照してください。
11	ランデブーポイントのグループアドレスに，中継対象グループアドレスが含まれていることを確認してください。 show ip pim rp-mapping	中継対象グループアドレスが含まれていない場合は，ランデブーポイントルータの設定を確認してください。ランデブーポイントが本装置の場合は，「(3) ランデブーポイントルータ確認内容」を参照してください。
12	マルチキャスト中継エントリが存在することを確認してください。 show ip mcache	マルチキャスト中継エントリが存在しない場合は，上流ポートにマルチキャストデータが届いていることを確認してください。マルチキャストデータが届いていない場合は，マルチキャスト送信者あるいは上流ルータの設定を確認してください。

項番	確認内容・コマンド	対応
13	マルチキャスト経路情報が存在することを確認してください。 show ip mroute	マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
14	マルチキャスト経路情報かマルチキャスト中継エントリが上限を超えていないか確認してください。 マルチキャスト経路情報： show ip mroute マルチキャスト中継エントリ： show ip mcache netstat multicast	Warning が出力されている場合は，想定していないマルチキャスト経路情報またはマルチキャスト中継エントリが作成されていないか確認してください。マルチキャスト中継エントリでネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。

(2) BSR 確認内容

次の表に，IPv4 PIM-SM ネットワーク構成で本装置が BSR の場合の確認内容を示します。

表 3-23　BSR 確認内容

項番	確認内容・コマンド	対応
1	本装置が BSR 候補であることを確認してください。 show ip pim bsr	本装置が BSR 候補でない場合はコンフィグレーションを確認し，BSR 候補として動作するように設定してください。また，loopback インタフェースにアドレスが設定されていないと BSR 候補として動作しないため，loopback インタフェースにアドレスが設定されていることも確認してください。
2	本装置が BSR であることを確認してください。 show ip pim bsr	本装置が BSR でない場合は，ほかの BSR 候補の優先度を確認してください。優先度は値の大きい方が高くなります。優先度が同じ場合は，BSR アドレスが一番大きい BSR 候補が BSR となります。

(3) ランデブーポイントルータ確認内容

次の表に，IPv4 PIM-SM ネットワーク構成で本装置がランデブーポイントルータの場合の確認内容を示します。

表 3-24　ランデブーポイントルータ確認内容

項番	確認内容・コマンド	対応
1	本装置が中継対象グループアドレスに対するランデブーポイント候補であることを確認してください。 show ip pim rp-mapping	本装置が中継対象グループアドレスに対するランデブーポイント候補でない場合は，コンフィグレーションを確認し，中継対象グループアドレスに対するランデブーポイント候補として動作するように設定してください。また，loopback インタフェースにアドレスが設定されていないとランデブーポイント候補として動作しないため，loopback インタフェースにアドレスが設定されていることも確認してください
2	本装置が中継対象グループアドレスに対するランデブーポイントであることを確認してください。 show ip pim rp-hash <Group Address>	本装置がランデブーポイントでない場合は，ほかのランデブーポイント候補の優先度を確認してください。優先度は値の小さい方が高くなります。ほかのランデブーポイント候補の優先度が高い場合はランデブーポイントとして動作せず，優先度が同一の場合は，プロトコルの仕様でグループアドレス単位に分散され，該当グループに対してランデブーポイントとして動作しないことがあります。本装置を優先的にランデブーポイントとして動作させる場合は，ほかのランデブーポイント候補より高い優先度を設定してください。

(4) last-hop-router 確認内容

次の表に，IPv4 PIM-SM ネットワーク構成で本装置が last-hop-router の場合の確認内容を示します。

表 3-25 last-hop-router 確認内容

項番	確認内容・コマンド	対応
1	マルチキャスト受信者と接続しているインタフェースで，IGMP が動作していることを確認してください。 show ip igmp interface	動作していない場合はコンフィグレーションを確認し，IGMP が動作するように設定してください。
2	マルチキャスト受信者が，IGMP で中継対象グループに参加していることを確認してください。 show ip igmp group	中継対象グループに参加していない場合は，マルチキャスト受信者の設定を確認してください。
3	中継対象グループが参加しているインタフェースがある場合は，本装置が DR であることを確認してください。 show ip pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を調査してください。
4	静的グループ参加機能が動作するインタフェースに，IGMP snooping が設定されているか確認してください。 show igmp-snooping	IGMP snooping が設定されている場合は，以下の内容を確認してください。 • 中継先ポートに対して IGMP snooping のマルチキャストルータポートの設定がされているか確認してください。 • 「3.6.4 IGMP snooping によるマルチキャスト中継ができない」を参照してください。
5	各インタフェースで異常を検出していないか確認してください。 show ip igmp interface	Notice を確認し，警告情報が出力されていないことを確認してください。 警告情報が出力されている場合は以下を確認してください。 • L：想定した最大数を超えて参加要求が発生しています。接続ユーザ数を確認してください。 • Q：隣接するルータと IGMP のバージョンが不一致となっています。IGMP のバージョンを合わせてください。 • R：現在の設定では受信できない Report を送信しているユーザが存在します。本装置の IGMP のバージョンを変更するか，参加ユーザの設定を確認してください。

(5) first-hop-router 確認内容

次の表に，IPv4 PIM-SM ネットワーク構成で本装置が first-hop-router の場合の確認内容を示します。

表 3-26 first-hop-router 確認内容

項番	確認内容・コマンド	対応
1	本装置がマルチキャスト送信者と直接接続していることを確認してください。	直接接続していない場合はネットワーク構成を確認してください。
2	マルチキャスト送信者と接続しているインタフェースで，PIM-SM または IGMP が動作していることを確認してください。 show ip pim interface show ip igmp interface	動作していない場合はコンフィグレーションを確認し，PIM-SM または IGMP が動作するように設定してください。
3	マルチキャスト経路情報が存在するか確認してください。 show ip mroute	マルチキャスト経路情報が存在しない場合は，マルチキャストデータ送信元アドレスが，マルチキャスト送信者と直接接続しているインタフェースのネットワークアドレスであることを確認してください。

3.9.2　IPv4 PIM-SM ネットワークでマルチキャストデータが二重中継される

IPv4 PIM-SM ネットワーク構成でマルチキャストデータが二重中継される場合は，各ルータの設定内容を確認し，同一ネットワークに複数のルータが存在するインタフェースでは PIM-SM が動作するように設定してください。

上記の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 3-27　二重中継が継続する場合の確認

項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの PIM の隣接情報を確認してください。 show ip pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM-SM が動作していることを show ip pim interface コマンドで確認してください。 • フィルタなどによるプロトコルパケットの中継を抑止する設定がないことを，コンフィグレーションで確認してください。フィルタ設定情報の確認手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。 • 隣接ルータの設定を確認してください。

3.9.3　IPv4 PIM-SSM ネットワークで通信ができない

IPv4 PIM-SSM ネットワーク構成でマルチキャスト中継ができない場合は，以下に示す障害解析方法に従って原因の切り分けを行ってください。

IPv4 PIM-SSM のネットワーク例を次の図に示します。

図 3-11　IPv4 PIM-SSM ネットワーク例

注

- first-hop-router：マルチキャスト送信者と直接接続するルータ
- last-hop-router：マルチキャスト受信者と直接接続するルータ

(1)　共通確認内容

次の表に，IPv4 PIM-SSM ネットワーク構成のすべての本装置に対する共通確認内容を示します。

表 3-28 共通確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションにマルチキャスト機能を使用する指定（ip multicast routing）があることを確認してください。 show running-config	マルチキャスト機能を使用する指定がない場合は，コンフィグレーションを修正してください。
3	一つ以上のインタフェースで PIM-SM が動作していることを確認してください。 show ip pim interface	動作していない場合はコンフィグレーションを確認し，どれか一つ以上のインタフェースで PIM-SM が動作するように設定してください。コンフィグレーションで PIM の動作設定をしたインタフェースが，show ip pim コマンドの interface パラメータ指定時に表示されない場合は，該当インタフェースにマルチホームの設定がされていないことを確認してください。
4	PIM が動作するインタフェースに，IGMP snooping が設定されているか確認してください。 show igmp-snooping	IGMP snooping が設定されている場合は，以下の内容を確認してください。 • 隣接ルータと接続しているポートに対して IGMP snooping のマルチキャストルータポートの設定がされているか確認してください。 • 「3.6.4 IGMP snooping によるマルチキャスト中継ができない」を参照してください。
5	PIM および IGMP が動作するインタフェースで，フィルタなどによるプロトコルパケットおよびマルチキャストパケット中継を抑止する設定がないことをコンフィグレーションで確認してください。 show running-config	プロトコルパケットおよびマルチキャストパケット中継を抑止する設定がある場合は，コンフィグレーションを修正してください。フィルタ設定情報の確認手順については，「3.22.1 フィルタ /QoS 設定情報の確認」を参照してください。
6	PIM の隣接情報を確認してください。 show ip pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ip pim で interface パラメータを指定して確認してください。 • 隣接ルータの設定を確認してください。
7	マルチキャストデータ送信者へのユニキャスト経路が存在するか確認してください。 show ip route	ユニキャスト経路が存在しない場合は，「3.8 IPv4 ユニキャストルーティングの通信障害」を参照してください。
8	マルチキャストデータ送信者へのユニキャスト経路送出インタフェースで，PIM が動作していることを確認してください。 show ip pim interface	動作していない場合はコンフィグレーションを確認し，ユニキャスト経路送出インタフェースで PIM が動作するように設定してください。
9	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていることを，コンフィグレーションで確認してください。 show running-config	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていない場合は，コンフィグレーションを修正してください。
10	マルチキャスト経路情報が存在するか確認してください。 show ip mroute	マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
11	マルチキャスト経路情報かマルチキャスト中継エントリが上限を超えていないか確認してください。 マルチキャスト経路情報： show ip mroute マルチキャスト中継エントリ： show ip mcache netstat multicast	Warning が出力されている場合は，想定していないマルチキャスト経路情報またはマルチキャスト中継エントリが作成されていないか確認してください。マルチキャスト中継エントリでネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。

(2) last-hop-router 確認内容

次の表に，IPv4 PIM-SSM ネットワーク構成で本装置が last-hop-router の場合の確認内容を示します。

表 3-29 last-hop-router 確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションに IGMPv1/IGMPv2 で PIM-SSM の連携動作が使用できる指定（ip igmp ssm-map enable）があることを確認してください。 show running-config	IGMPv1/IGMPv2 で PIM-SSM の連携動作が使用できる指定がない場合は，コンフィグレーションを修正してください。
2	コンフィグレーションに PIM-SSM で中継するグループアドレスと送信元アドレスが，IGMPv1/IGMPv2 で PIM-SSM と連携動作する設定（ip igmp ssm-map static）があることを確認してください。 show running-config	IGMPv1/IGMPv2 で PIM-SSM と連携動作する設定がない場合は，コンフィグレーションを修正してください。
3	マルチキャスト受信者と接続しているインタフェースで IGMP が動作していることを確認してください。 show ip igmp interface	動作していない場合は，コンフィグレーションを確認し IGMP が動作するように設定してください。
4	マルチキャスト受信者が IGMP で中継対象グループに参加していることを確認してください。 show ip igmp group	中継対象グループにグループ参加していない場合は，マルチキャスト受信者の設定を確認してください。
5	中継対象グループが参加しているインタフェースがある場合は，本装置が DR であることを確認してください。 show ip pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を調査してください。
6	静的グループ参加機能が動作するインタフェースに，IGMP snooping が設定されているか確認してください。 show igmp-snooping	IGMP snooping が設定されている場合は，以下の内容を確認してください。 • 中継先ポートに対して IGMP snooping のマルチキャストルータポートの設定がされているか確認してください。 • 「3.6.4 IGMP snooping によるマルチキャスト中継ができない」を参照してください。
7	各インタフェースで異常を検出していないか確認してください。 show ip igmp interface	Notice を確認し，警告情報が出力されていないことを確認してください。 警告情報が出力されている場合は以下を確認してください。 • L：想定した最大数を超えて参加要求が発生しています。接続ユーザ数を確認してください。 • Q：隣接するルータと IGMP のバージョンが不一致となっています。IGMP のバージョンを合わせてください。 • R：現在の設定では受信できない Report を送信しているユーザが存在します。本装置の IGMP のバージョンを変更するか，参加ユーザの設定を確認してください。 • S：IGMPv3 で 1 メッセージ内に格納できるソース数が上限を超えたため参加情報を一部廃棄しています。参加ユーザの設定を確認してください。

(3) first-hop-router 確認内容

次の表に，IPv4 PIM-SSM ネットワーク構成で本装置が first-hop-router の場合の確認内容を示します。

表 3-30 first-hop-router 確認内容

項番	確認内容・コマンド	対応
1	本装置がマルチキャスト送信者と直接接続していることを確認してください。	直接接続していない場合はネットワーク構成を確認してください。

項番	確認内容・コマンド	対応
2	マルチキャスト送信者と接続しているインタフェースで，PIM-SM または IGMP が動作していることを確認してください。 show ip pim interface show ip igmp interface	動作していない場合はコンフィグレーションを確認し，PIM-SM または IGMP が動作するように設定してください。
3	マルチキャストデータが本装置に届いているか確認してください。	マルチキャストデータが届いていない場合は，マルチキャスト送信者の設定を確認してください。
4	マルチキャストデータとマルチキャスト経路情報のグループアドレスと送信元アドレスが一致するか確認してください。 show ip mroute show netstat multicast	グループアドレスと送信元アドレスが一致しない場合は，マルチキャスト送信者と last-hop-router の設定内容を確認してください。

3.9.4 IPv4 PIM-SSM ネットワークでマルチキャストデータが二重中継される

IPv4 PIM-SSM ネットワーク構成でマルチキャストデータが二重中継される場合は，各ルータの設定内容を確認し，同一ネットワークに複数のルータが存在するインタフェースでは PIM-SM が動作するように設定してください。

上記の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 3-31 二重中継が継続する場合の確認内容

項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの PIM の隣接情報を確認してください。 show ip pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM-SM が動作していることを show ip pim コマンドで interface パラメータを指定して確認してください。 • フィルタなどによるプロトコルパケットの中継を抑止する設定がないことを，コンフィグレーションで確認してください。フィルタ設定情報の確認手順については，「3.22.1 フィルタ /QoS 設定情報の確認」を参照してください。 • 隣接ルータの設定を確認してください。

3.9.5 VRF での IPv4 マルチキャスト通信のトラブル

VRF での IPv4 マルチキャスト通信のトラブルは，以下の確認を行ってください。

表 3-32 VRF での確認内容

項番	確認内容・コマンド	対応
1	VRF のインタフェースが正しいか，ポート番号および VLAN ID を確認してください。 show ip vrf show vlan show ip pim interface	正しくない場合はコンフィグレーションまたは接続を修正してください。

項番	確認内容・コマンド	対応
3	本装置がランデブーポイントまたは BSR の場合，該当 VRF に loopback インタフェースが設定されているかコンフィグレーションを確認してください。 show ip vrf show running-config	ランデブーポイントまたは BSR に指定した loopback インタフェース番号を，該当 VRF の loopback インタフェース番号と同じにしてください。 また，その loopback インタフェースに IPv4 アドレスが設定されていない場合は，IPv4 アドレスを設定してください。
4	複数の VRF で運用している場合，グローバルネットワークまたは特定の VRF がマルチキャスト中継エントリを想定以上に占有していないか確認してください。 show ip mcache vrf all	ネットワーク設計の想定以上にマルチキャスト中継エントリを占有しているグローバルネットワークまたは VRF があった場合は，想定していないマルチキャスト中継エントリが作成されていないか確認してください。 ネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。 また，VRF ごとの中継エントリの最大数を設定して一つのグローバルネットワークまたは特定の VRF が中継エントリを占有しないようにしてください。 該当するコンフィグレーション： ip pim vrf <vrf id> mcache-limit <number>
5	各 VRF に対し，「3.9.1　IPv4 PIM-SM ネットワークで通信ができない」～「3.9.4　IPv4 PIM-SSM ネットワークでマルチキャストデータが二重中継される」の確認をしてください。	情報確認のための各コマンドは VRF を指定する必要があります。VRF 指定の方法は，マニュアル「運用コマンドレファレンス」を参照してください。

3.9.6 エクストラネットでの IPv4 マルチキャスト通信のトラブル

エクストラネットでの IPv4 マルチキャスト通信のトラブルは，まず，「3.9.5　VRF での IPv4 マルチキャスト通信のトラブル」を確認し，各 VRF でマルチキャスト通信ができることを確認してください。次に，以下の確認を行ってください。

表 3-33　エクストラネットでの確認内容

項番	確認内容・コマンド	対応
1	中継先 VRF から送信元のアドレスへのユニキャスト経路が，期待する VRF またはグローバルネットワークであることを確認してください。 show ip rpf	正しくない場合はユニキャストエクストラネットの設定を見直してください。
2	エクストラネットで使用する IPv4 マルチキャストアドレスに対応するプロトコル（PIM-SM または PIM-SSM）が，中継先 VRF と上流側 VRF で同じであることを確認してください。 show running-config	プロトコルが異なる場合は，中継先 VRF と上流側 VRF で同じプロトコルとなる IPv4 マルチキャストアドレスを使用してください。
3	上流側 VRF で，送信元アドレスへのユニキャスト経路が，さらに別の VRF になっていないか確認してください。 show ip rpf	上流側 VRF で，送信元アドレスへのユニキャスト経路がその VRF 内の実インタフェースである VRF となるようにしてください。
4	PIM-SM VRF ゲートウェイを使用する場合，上流側 VRF に (*,G) エントリが生成されていることを確認してください。また，該当する (*,G) エントリの表示項目 Flags に "V" が表示されていることを確認してください。 show ip mroute	(*,G) エントリが正常に生成されていない場合，上流側 VRF の IPv4 マルチキャスト経路フィルタリングにエクストラネット通信で使用する IPv4 マルチキャストアドレスが，ホストアドレス指定で許可されていることを確認してください。

項番	確認内容・コマンド	対応
5	PIM-SM VRF ゲートウェイを使用する場合，上流側 VRF で生成された (*,G) エントリの下流インタフェースに中継先 VRF が表示されていることを確認してください。 show ip mroute	上流側 VRF の (*,G) エントリの downstream に中継先 VRF が存在しない場合，上流側 VRF の IPv4 マルチキャスト経路フィルタリングのホストアドレス指定をしている route-map に，中継先 VRF が許可されていることを確認してください。 なお，route-map の match vrf による個別 VRF 指定がない場合は，すべての VRF が中継先として許可されています。
6	show ip mroute で上流インタフェースの VRF 表示に "(denied)" が表示されている場合は，上流側 VRF の IPv4 マルチキャスト経路フィルタリングが正しく設定されていません。経路がない場合は，コンフィグレーションで上流側 VRF の IPv4 マルチキャスト経路フィルタリングを確認してください。 show ip mroute show running-config	上流側 VRF の IPv4 マルチキャスト経路フィルタリングにエクストラネット通信で使用する IPv4 マルチキャストアドレスと中継先 VRF を許可していることを確認してください。 なお，IPv4 マルチキャスト経路フィルタリングに IPv4 マルチキャストアドレスおよび VRF が個別指定されていない場合は，IPv4 マルチキャストアドレスおよび VRF のすべてが許可されています。

3.10　IPv6 ネットワークの通信障害

3.10.1　通信できない，または切断されている

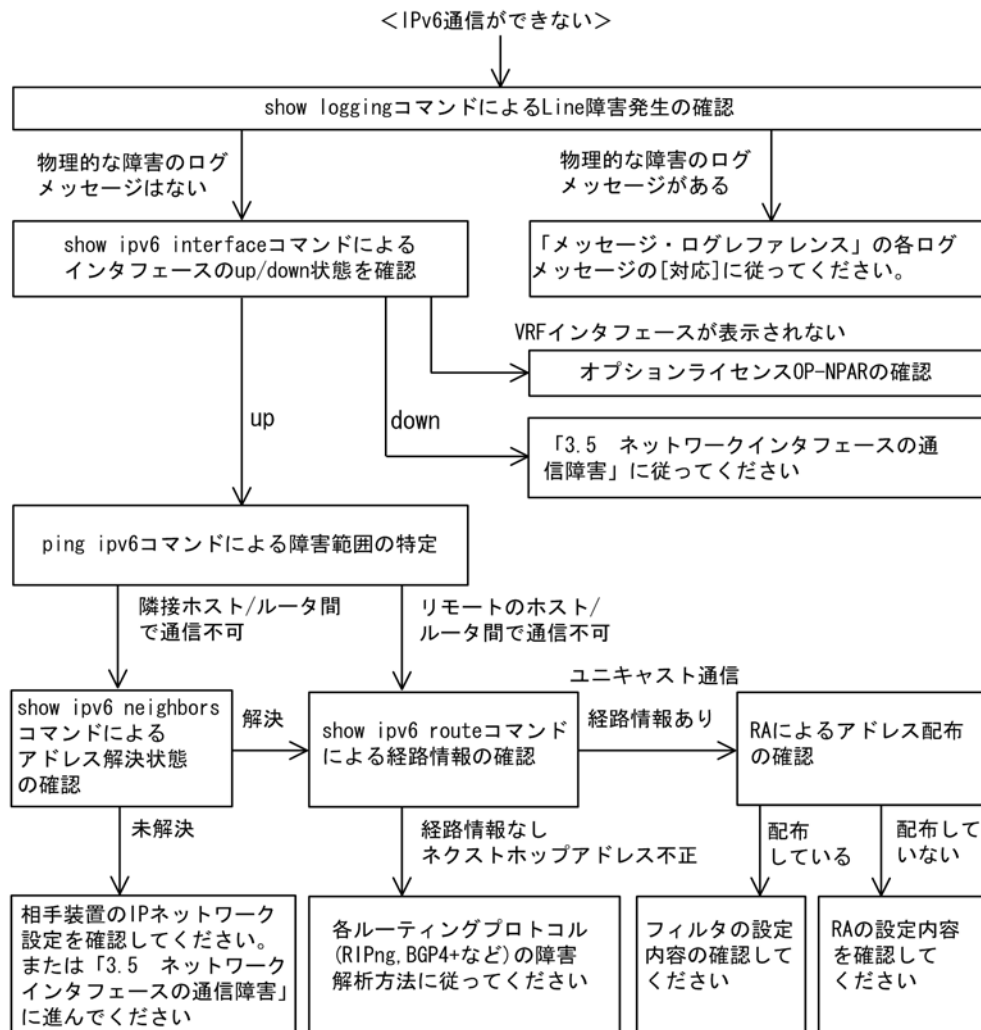
本装置を使用している IPv6 ネットワーク上で，通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. IPv6 通信に関係するコンフィグレーションの変更
2. ネットワークの構成変更
3. ネットワークを構成する機器の障害

上記 1. および 2. については，コンフィグレーションおよびネットワーク構成の変更前と変更後の差分を調べていただき，通信ができなくなるような原因がないか確認してください。

ここでは，3. に示すように「コンフィグレーションおよびネットワーク構成は正しいのに IPv6 通信ができない」，「これまで正常に動いていたのに IPv6 通信ができなくなった」というケースを中心に，障害部位および原因の切り分け手順を説明いたします。

障害部位および原因の切り分け方法は，次のフローに従ってください。

図 3-12 IPv6 通信ができない場合の障害解析手順

(1) ログの確認

通信ができなくなる原因の一つには，回線の障害（または壊れ）が考えられます。本装置が表示するログで，ハードウェアの障害を示すメッセージの表示手順を示します。

なお，ログの内容については，マニュアル「メッセージ・ログレファレンス」を参照してください。

1. 本装置にログインします。
2. show logging コマンドを使ってログを表示させます。
3. ログには各々発生した日時が表示されます。通信ができなくなった日時にログが表示されていないか確認してください。
4. 通信ができなくなった日時に表示されているログの障害の内容および障害への対応については，マニュアル「メッセージ・ログレファレンス」に記載しています。その指示に従ってください。
5. 通信ができなくなった日時にログの表示がないときは，「(2) インタフェース状態の確認」に進んでください。

(2) インタフェース状態の確認

本装置のハードウェアは正常に動作している場合でも，本装置と接続している隣接の装置のハードウェアに障害が発生していることも考えられます。

本装置と隣接の装置間の，インタフェースの状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ipv6 interface コマンドを使って該当装置間のインタフェースの Up ／ Down 状態を確認してください。
3. 該当インタフェースが”Down”状態のときは，「3.5　ネットワークインタフェースの通信障害」を参照してください。
4. 該当インタフェースとの間のインタフェースが”Up”状態のときは，「(3) 障害範囲の特定（本装置から実施する場合)」に進んでください。

(3) 障害範囲の特定（本装置から実施する場合）

本装置に障害がない場合は，通信を行っていた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping ipv6 コマンドを使って通信できない両方の相手との疎通を確認してください。ping ipv6 コマンドの操作例および実行結果の見方については，マニュアル「コンフィグレーションガイド」を参照してください。
3. ping ipv6 コマンドで通信相手との疎通が確認できなかった場合は，さらに ping ipv6 コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping ipv6 コマンド実行の結果，障害範囲が隣接装置の場合は「(5) 隣接装置との NDP 解決情報の確認」に，リモート先の装置の場合は「(6) ユニキャストインタフェース情報の確認」に進んでください。

(4) 障害範囲の特定（お客様の端末装置から実施する場合）

本装置にログインできない環境にある場合に，お客様の端末装置から通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. お客様の端末装置に ping ipv6 機能があることを確認してください。
2. ping ipv6 機能をお使いになり，お客様の端末装置と通信相手との疎通ができるか確認してください。
3. ping ipv6 機能で通信相手との疎通が確認できなかった場合は，さらに ping ipv6 コマンドを使ってお客様の端末装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping ipv6 機能による障害範囲が特定できましたら，障害と考えられる装置が本装置である場合は本装置にログインしていただき，障害解析フローに従って障害原因の調査を行ってください。

(5) 隣接装置との NDP 解決情報の確認

ping ipv6 コマンドの実行結果によって隣接装置との疎通が不可の場合は，NDP によるアドレスが解決していないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。
2. show ipv6 neighbors コマンドを使って隣接装置間とのアドレス解決状態（NDP エントリ情報の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（NDP エントリ情報あり）場合は，「(6) ユニキャストインタフェース情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（NDP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が一致しているかを確認してください。

(6) ユニキャストインタフェース情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信ができない場合や，IPv6 ユニキャスト通信で通

信相手との途中の経路で疎通が不可となる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ipv6 route コマンドを実行して，本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は「3.11 IPv6 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - RA 機能
   「(8) RA 設定情報の確認」に進んでください。

(7) フィルタ /QoS 設定情報の確認

フィルタによって特定のパケットが廃棄されているか，QoS 制御の帯域監視，廃棄制御またはシェーパによってパケットが廃棄されている可能性があります。

コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システムの構築での帯域監視ならびに廃棄制御・シェーパのシステム運用が適切であるか見直してください。手順については，「3.22.1 フィルタ /QoS 設定情報の確認」を参照してください。

(8) RA 設定情報の確認

本装置と本装置に直接接続されている端末との間で通信ができない場合は，RA によるアドレス情報配布が正常に行われていない可能性が考えられます。したがって，コンフィグレーションの RA 機能の設定が正しいか確認してください。確認手順を次に示します。

1. 本装置にログインします。
2. show ipv6 routers コマンドを実行して，本装置の RA 情報を確認してください。
3. IPv6 アドレス情報が正しく配布されていた場合，通信不可のインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - フィルタ／ QoS 機能
   「(7) フィルタ /QoS 設定情報の確認」を参照してください。

3.10.2 IPv6 DHCP リレーの通信トラブル

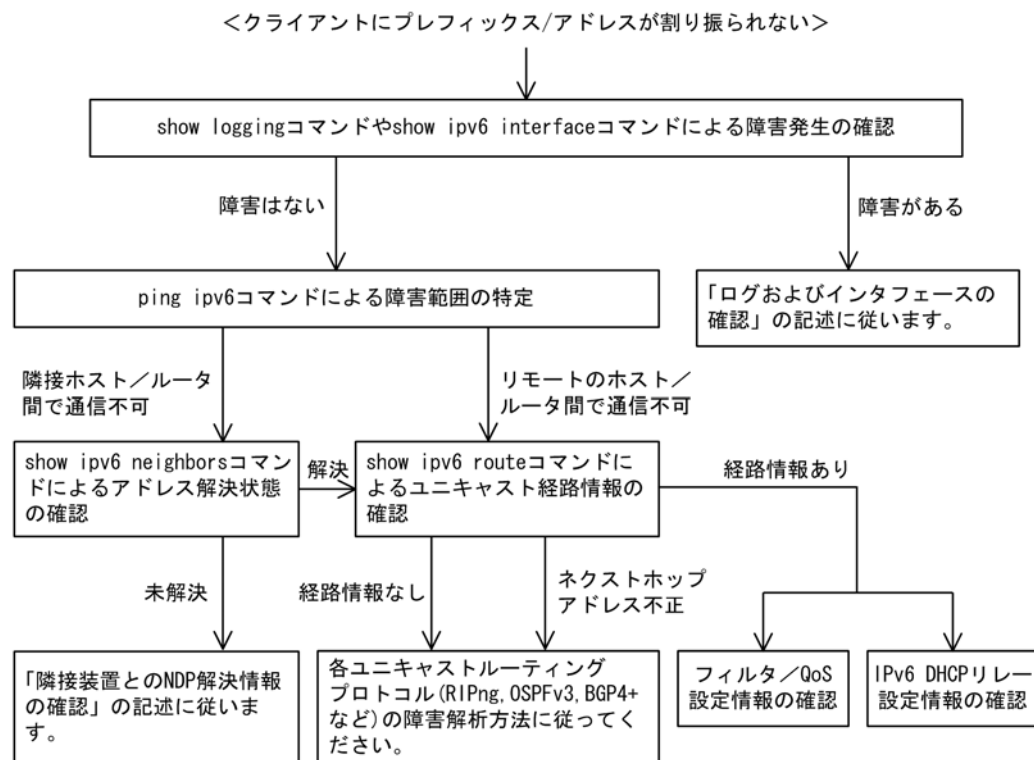
IPv6 DHCP リレーの通信トラブルが発生する要因として考えられるのは，次の 3 種類があります。

1. IPv6 DHCP リレーに関するコンフィグレーションの変更
2. ネットワーク構成変更
3. IPv6 DHCP サーバの障害

上記 2. については，ネットワーク構成の変更前と変更後の差分を調べ，通信ができなくなるような原因がないか確認してください。

ここでは，クライアントの設定は確認されているものとし，上記 1. および 3. に示す「コンフィグレーションを変更したあと，IPv6 DHCP サーバから情報が配布されなくなった」および「コンフィグレーションおよびネットワーク構成は正しいのに，クライアントにプレフィックス（アドレス）が割り振られないため，IP 通信ができない」というケースについて，障害部位および原因の切り分け手順を示します。

障害部位および原因の切り分け方法は，次のフローに従ってください。

図 3-13　IPv6 DHCP リレーの障害解析手順

(1)　ログおよびインタフェースの確認

クライアントにプレフィックス / アドレスが割り振られなくなる原因の一つにクライアント－サーバ間で通信ができなくなっていることが考えられます。本装置が表示するログや show ipv6 interface コマンドによるインタフェースの up ／ down 状態を確認してください。手順については「3.10.1　通信できない，または切断されている」を参照してください。

(2)　障害範囲の特定

本装置に障害がない場合は，通信していた相手との間のどこかに障害が発生している可能性があります。通信相手とのどこの部分で障害が発生しているか障害範囲を特定する手順を次に示します。

1. 本装置にログインします。
2. ping ipv6 コマンドを使って通信できない両方の相手との疎通を確認してください。ping ipv6 コマンドの操作例および実行結果の見方は「コンフィグレーションガイド」を参照してください。
3. ping ipv6 コマンドで通信相手との疎通が確認できなかった場合は，さらに ping ipv6 コマンドを使って本装置に近い装置から順に通信相手に向けて疎通を確認してください。
4. ping ipv6 コマンド実行の結果，障害範囲が隣接装置の場合は「(3)　隣接装置との NDP 解決情報の確認」に，リモート先の装置の場合は「(4)　ユニキャスト経路情報の確認」に進んでください。

(3)　隣接装置との NDP 解決情報の確認

ping ipv6 コマンドによって隣接装置との疎通が確認できないときは，NDP によるアドレスが解決できていないことが考えられます。本装置と隣接装置間のアドレス解決状態を確認する手順を次に示します。

1. 本装置にログインします。

2. show ipv6 neighbors コマンドを使って隣接装置間とのアドレス解決状態（NDP エントリ状態の有無）を確認してください。
3. 隣接装置間とのアドレスが解決している（NDP エントリ情報あり）場合は，「(4) ユニキャスト経路情報の確認」に進んでください。
4. 隣接装置間とのアドレスが解決していない（NDP エントリ情報なし）場合は，隣接装置と本装置の IP ネットワーク設定が疎通できる設定になっているかを確認してください。

(4) ユニキャスト経路情報の確認

隣接装置とのアドレスが解決しているにもかかわらず通信できない，通信相手との途中の経路で疎通できなくなる，または通信相手までの経路がおかしいなどの場合は，本装置が取得した経路情報を確認する必要があります。確認手順を次に示します。

1. 本装置にログインします。
2. show ipv6 route コマンドを使って本装置が取得した経路情報を確認してください。
3. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がない場合やネクストホップアドレスが不正の場合は，「3.11　IPv6 ユニキャストルーティングの通信障害」に進んでください。
4. 本装置が取得した経路情報の中に，通信障害となっているインタフェースの経路情報がある場合は，通信できないインタフェースに設定している次の機能に問題があると考えられます。該当する機能の調査を行ってください。
   - フィルタ／ QoS 機能
     「(5) フィルタ /QoS 設定情報の確認」に進んでください。
   - IPv6 DHCP リレー
     「(6) IPv6 DHCP リレー設定情報の確認」に進んでください。

(5) フィルタ /QoS 設定情報の確認

本装置で，物理的障害がなく，経路情報も正しく設定されているにもかかわらず通信できない場合は，フィルタによって特定のパケットだけを廃棄する設定になっているか，QoS 制御の帯域監視，廃棄制御またはシェーパによってパケットが廃棄されている可能性があります。

したがって，コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築での帯域監視，廃棄およびシェーパのシステム運用が適切であるかを確認してください。手順については「3.22　フィルタ /QoS の設定により生じる通信障害」を参照してください。

(6) IPv6 DHCP リレー設定情報の確認

IPv6 DHCP サーバに貸し出し用プレフィックス / アドレスが十分に残っている場合，IPv6 DHCP リレーのコンフィグレーションの設定誤りによってクライアントにプレフィックス / アドレスが割り振られなかったという原因が考えられます。

次にコンフィグレーションの確認手順を示します。

1. コンフィグレーションコマンド ipv6 dhcp relay destination には，IPv6 DHCP サーバもしくは IPv6 DHCP リレーの IPv6 アドレス，または IPv6 DHCP サーバの存在するネットワークへのインタフェースが設定されているか確認してください。
2. クライアント側のインタフェースにコンフィグレーションコマンド ipv6 dhcp relay destination が設定されているか確認してください。
3. 該当クライアントへプレフィックス / アドレスを貸与させたい IPv6 DHCP サーバの IPv6 アドレス（またはインタフェース）が，コンフィグレーションコマンド ipv6 dhcp relay destination で設定されているかを確認してください。

4. コンフィグレーションコマンド ipv6 dhcp relay hop-limit に設定している hop-limit 値がクライアントから見て正しい hop 値以上となっているかを確認してください。

3.10.3 IPv6 DHCP サーバに関するトラブルシューティング

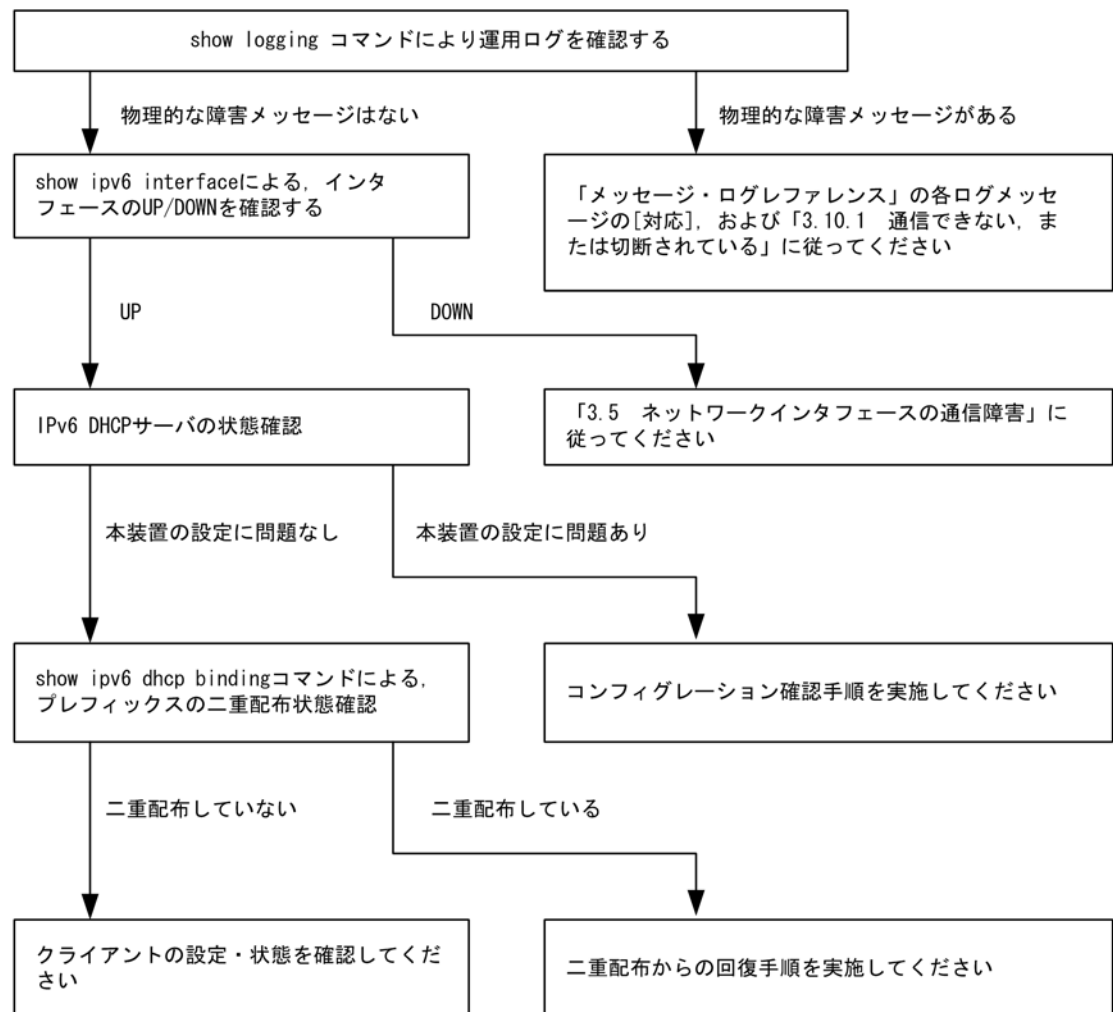
(1) コンフィグレーションが配布されない

本装置 IPv6 DHCP サーバのプレフィックス配布機能を使用するに当たり，サービスが正常に動作しない原因としては，以下の 5 点が考えられます。

1. プレフィックス配布設定数に対して，クライアント数が多い。
2. クライアント DUID（DHCP Unique Identifier）の指定を誤っている。
3. ipv6 dhcp server 設定を誤っている。
4. IPv6 DHCP サーバ運用中の障害
5. その他の障害

上記は，以下の手順で障害個所を切り分け，確認できます。

図 3-14 IPv6 DHCP サーバの障害解析手順

<コンフィグレーションが配布できない>

(a) ログおよびインタフェースの確認

通信ができなくなる原因として，NIM，インタフェースの障害（または壊れ）や，隣接装置の障害が考えられます。本装置が表示するログや，show ipv6 interface コマンドによるインタフェースの up/down 状態を確認してください。手順については「3.10.1　通信できない，または切断されている」を参照してください。

(b) 本装置の IPv6 DHCP サーバ状態確認

1. IPv6 DHCP サーバサービスの起動確認
   show ipv6 dhcp server statistics コマンドで，IPv6 DHCP サーバデーモンから情報が取得できるか確認してください。show ipv6 dhcp server statistics コマンドの実行結果が以下の場合は，コンフィグレーションコマンド service ipv6 dhcp で IPv6 DHCP サーバ機能を再設定してください。

   [実行結果]

```
> show ipv6 dhcp server statistics
> < show statistics >: dhcp6_server doesn't seem to be running.
```

2. 配布可能なプレフィックスの残数を確認する
   show ipv6 dhcp server statistics コマンドで，IPv6 DHCP サーバがあといくつプレフィックスを配布できるかを確認してください。確認手順については，マニュアル「コンフィグレーションガイド」を参照してください。確認の結果，配布可能なプレフィックス数が 0 である場合は配布するプレフィックス数を増やしてください。なお，配布可能なプレフィックス数の上限は 1024 です。

(c) コンフィグレーション確認手順

1. IPv6 DHCP サーバ機能の有効設定の確認
   コンフィグレーションコマンド show service で，IPv6 DHCP サーバ設定が有効になっているかを確認してください。実行結果で示す下線部が表示されなければ IPv6 DHCP サーバ機能は有効です。

   [実行結果]

```
(config)# show service
no service ipv6 dhcp
!
(config)#
```

2. ipv6 dhcp server の設定を確認する
   コンフィグレーションコマンド show で，ipv6 dhcp server 設定の有無を確認してください。設定がない場合は追加してください。設定がある場合は，設定しているインタフェースが，クライアント接続ネットワーク向けの設定であることを確認してください。

   [実行結果]

```
(config)# show
interface vlan 10
  ipv6 address 3ffe:1:2:: linklocal
  ipv6 enable
  ipv6 dhcp server Tokyo preference 100
!
(config)#
```

3. ipv6 dhcp pool ／ ipv6 local pool ／ prefix-delegation ／ prefix-delegation pool の設定を確認する
   コンフィグレーションコマンド show ipv6 dhcp で，IPv6 DHCP サーバで配布しようとしているプレフィックス配布設定の有無を確認してください。設定がない場合は追加してください。設定がある場合は，配布するプレフィックスを指定する prefix-delegation ／ ipv6 local pool の設定値，配布クライアントを決める duid の設定有無，ならびに duid に指定したクライアント DUID の値が正しいかを確認してください。

[実行結果]

```
(config)# show ipv6 dhcp
ipv6 dhcp pool Tokyo
  prefix-delegation 3ffe:1:2::/48 00:03:00:01:11:22:33:44:55
!
(config)#
```

(d) クライアントによる二重取得

1. binding 情報の確認

   show ipv6 dhcp binding コマンドを detail パラメータ指定で実行し，同一 DUID に対してプレフィックスが二重に配布されていないかを確認します。以下に表示例を示します。

   [実行結果]

```
> show ipv6 dhcp binding detail
Total: 2 prefixes
<Prefix>             <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48      05/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48      05/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

   下線で示すように，同一 DUID が 2 個以上存在する場合は，プレフィックス情報を不当に取得しているクライアントである可能性があります。各クライアントを確認し，配布を受けたプレフィックス値を確認してください。

2. 配布済みプレフィックスとクライアントの対応をとる

   show ipv6 dhcp binding detail の結果で，プレフィックスを二重取得しているクライアントが見つからない場合は，表示される DUID とクライアント装置の対応を取る手順が必要となります。対応付けは，binding 情報に示される「配布済みプレフィックスの値」と「クライアント装置が配布を受けたプレフィックスの情報」を比較することで確認してください。

(e) クライアントの設定状態を確認する

クライアントの設定状態を確認する場合は，クライアント付属のマニュアルに従ってください。

(f) 二重配布からの回復手順

本装置 IPv6 DHCP サーバで，同一クライアントへプレフィックスを二重配布したことを確認した場合は，表示される DUID とクライアントの対応から，現在未使用のプレフィックスを調査してください。現在未使用のプレフィックスについては，clear ipv6 dhcp binding < 未使用プレフィックス > コマンドによって，binding 情報を削除してください。

[実行結果]

```
> show ipv6 dhcp binding detail
Total: 2 prefixes
<Prefix>             <Lease expiration>  <Type>
  <DUID>
3ffe:1234:5678::/48      05/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
3ffe:aaaa:1234::/48      05/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
> clear ipv6 dhcp binding 3ffe:1234:5678::/48
> show ipv6 dhcp binding detail
<Prefix>             <Lease expiration>  <Type>
  <DUID>
3ffe:aaaa:1234::/48      05/04/01 11:29:00   Automatic
  00:01:00:01:55:55:55:55:00:11:22:33:44:55
>
```

(2) プレフィックス配布先への通信ができない

本装置 DHCP サーバのプレフィックス配布先への自動経路情報設定機能を利用する場合，経路情報が設定されない要因は以下の二つがあります。

1. コンフィグレーション設定済みだが，未配布である。
2. 自動経路情報設定に関連する機能に影響がある操作，またはイベントが発生した。

上記は経路情報を確認する show ipv6 route -s コマンドの結果と show ipv6 dhcp server binding コマンドでの配布済みプレフィックス情報を比較することで切り分けることができます。

表 3-34　プレフィックス配布先への経路情報関連障害切り分け

条件		発生要因
binding 情報	経路情報	
あり	経路あり	該当なし。active 状態。
あり	経路なし	要因 2
なし	経路あり	要因 2
なし	経路なし	要因 1，2

プレフィックス配布先への経路情報の保有性については，次の表に示す制限があります。

表 3-35　プレフィックス配布先への経路情報の保有性

プレフィックスに関する保有情報	発生イベントと保有性			
	サーバ機能再起動		ルーティングマネージャ再起動	本装置再起動
	コマンド実行	サーバ障害		
クライアントへの経路情報	○	△	○	×

（凡例）
　○：保証される
　△：保証されない（各状態の情報が保有される場合もある）
　×：保証されない（初期化されるため，再設定要）

注
　プレフィックス配布先への経路情報設定を行う際に必要な経路管理機能
　なお，その他の障害については，「3.10.1　通信できない，または切断されている」を参照してください。

(a) 経路情報の確認

本装置 IPv6 DHCP サーバのプレフィックス配布先への自動経路設定機能を利用する場合，プレフィックス配布後の経路情報は，show ipv6 route コマンドで -s パラメータを指定して確認できます。

図 3-15 運用コマンドによる経路情報の確認

```
> show ipv6 route -s
Total: 10routes
Destination             Next Hop       Interface        Metric  Protocol  Age
3ffe:1234:5678::/48     ::1            tokyo            0/0      Static   45m
        <Active Gateway Dhcp>
3ffe:aaaa:1234::/48     ::1            osaka            0/0      Static   23m
        <Active Gateway Dhcp>
 :
>
```

(b) 経路情報の再設定を行う

本装置 IPv6 DHCP サーバのプレフィックス配布先への自動経路設定機能を利用する場合，障害などで経路情報がクリアされるイベントが発生したとき，その復旧にはプレフィックスの再配布が必要です。クライアント装置で，プレフィックス情報を再取得する操作を行ってください。

(3) 本装置 DUID が他装置と重複した場合

本装置を含む IPv6 DHCP サーバを同一ネットワーク上で 2 台以上運用する構成で，DUID が重複する場合は，以下の手順で本装置の DUID を再設定してください。

(a) DUID 情報保存ファイルを削除する

本装置 DUID は /usr/var/dhcp6/dhcp6s_duid に保存されています。運用コマンドラインより，rm コマンドを使用し，明示的に削除してください。

(b) DUID を再生成させる

DUID ファイルを削除後は，restart ipv6-dhcp server コマンドによって再起動させるか，コンフィグレーションへ IPv6 DHCP サーバ設定を追加してください。本装置 IPv6 DHCP サーバは起動時に IPv6 DHCP サーバインタフェースとして使用する ipv6 インタフェースの MAC アドレスを取得し，これと時刻情報を基に新たに生成します。

(c) DUID の確認

show ipv6 dhcp server statistics コマンドの「< Server DUID >」の項目によって確認できます。詳細は，マニュアル「コンフィグレーションガイド」を参照してください。

3.11 IPv6 ユニキャストルーティングの通信障害

3.11.1 RIPng 経路情報が存在しない

本装置が取得した経路情報の表示に，RIPng の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

また，ネットワーク・パーティションを使用していて，コンフィグレーションコマンド maximum routes で経路の上限値を設定している場合，まず「3.11.4　VRF で IPv6 経路情報が存在しない」の障害解析方法に従ってください。

表 3-36　RIPng の障害解析方法

項番	確認内容・コマンド	対応
1	RIPng の隣接情報を表示します。 show ipv6 rip neighbor	隣接ルータのインタフェースが表示されていない場合は項番 2 へ。
		隣接ルータのインタフェースが表示されている場合は項番 3 へ。
2	コンフィグレーションで RIPng 設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが RIPng 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。フィルタ設定情報の確認手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

3.11.2 OSPFv3 経路情報が存在しない

本装置が取得した経路情報の表示に，OSPFv3 の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

また，ネットワーク・パーティションを使用していて，コンフィグレーションコマンド maximum routes で経路の上限値を設定している場合，まず「3.11.4　VRF で IPv6 経路情報が存在しない」の障害解析方法に従ってください。

表 3-37　OSPFv3 の障害解析方法

項番	確認内容・コマンド	対応
1	OSPFv3 のインタフェース状態を確認します。 show ipv6 ospf interface <Interface Name>	インタフェース状態が DR または P to P の場合は項番 3 へ。
		インタフェース状態が BackupDR または DR Other の場合は項番 2 へ。
		インタフェースの状態が Waiting の場合は，時間を置いてコマンドを再実行してください。項番 1 へ。
2	Neighbor List 内より DR との隣接ルータ状態を確認します。	DR との隣接ルータ状態が Full 以外の場合は項番 4 へ。
		DR との隣接ルータ状態が Full の場合は項番 5 へ。

項番	確認内容・コマンド	対応
3	Neighbor List 内より全隣接ルータとの状態を確認します。	一部の隣接ルータ状態が Full 以外の場合は項番 4 へ。
		全隣接ルータ状態が Full の場合は項番 5 へ。
4	コンフィグレーションで OSPFv3 の設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 5 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
5	OSPFv3 経路を学習している経路を確認してください。 show ipv6 route all-routes	経路が InActive の場合には項番 6 へ。
		経路が存在しない場合は隣接ルータが OSPFv3 経路を広告しているか確認してください。
6	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが OSPFv3 経路を広告しているか確認してください。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。フィルタ設定情報の確認手順については,「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

3.11.3　BGP4+ 経路情報が存在しない

本装置が取得した経路情報の表示に，BGP4+ の経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

また，ネットワーク・パーティションを使用していて，コンフィグレーションコマンド maximum routes で経路の上限値を設定している場合，まず「3.11.4　VRF で IPv6 経路情報が存在しない」の障害解析方法に従ってください。

表 3-38　BGP4+ の障害解析方法

項番	確認内容・コマンド	対応
1	BGP4+ のピア状態を確認します。 show ipv6 bgp neighbors	ピア状態が Established 以外の場合は項番 2 へ。
		ピア状態が Established の場合は項番 3 へ。
2	コンフィグレーションで BGP4+ の設定が正しいか確認してください。	コンフィグレーションが正しい場合は項番 3 へ。
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。
3	BGP4+ 経路を学習しているか確認してください。 show ipv6 bgp received-routes	経路が存在するが active 状態でない場合は項番 4 へ。
		経路が存在しない場合は項番 5 へ。
4	BGP4+ 経路のネクストホップアドレスを解決する経路情報が存在するか確認してください。 show ipv6 route	ネクストホップアドレスを解決する経路情報がある場合は項番 5 へ。
		ネクストホップアドレスを解決する経路情報がない場合は，その経路情報を学習するためのプロトコルの障害解析を実施してください。
5	コンフィグレーションで経路をフィルタリングしていないか確認してください。	隣接ルータが BGP4+ 経路を広告しているか確認してください。

項番	確認内容・コマンド	対応
		コンフィグレーションが正しくない場合はコンフィグレーションを修正してください。フィルタ設定情報の確認手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。

3.11.4　VRF で IPv6 経路情報が存在しない

本装置が取得した経路情報の表示に，各プロトコルの経路情報が存在しない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-39　VRF の障害解析方法

項番	確認内容・コマンド	対応
1	VRF 内の経路数がコンフィグレーションで設定した上限値以上でないか確認してください。 show ipv6 vrf	経路数が上限値以上であれば項番 2 へ。
		経路数が上限値未満であれば，存在しない経路のプロトコルの障害解析を実施してください。 RIPng :「3.11.1　RIPng 経路情報が存在しない」 OSPFv3 :「3.11.2　OSPFv3 経路情報が存在しない」 BGP4+ :「3.11.3　BGP4+ 経路情報が存在しない」
2	コンフィグレーションで VRF 内の経路数の上限値を確認してください。	上限値を増やすか，経路を集約するなどして，経路数を減らしてください。

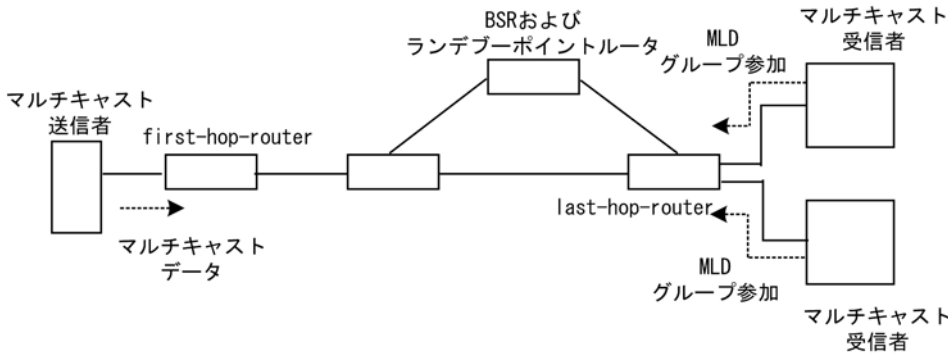
3.12 IPv6 マルチキャストルーティングの通信障害

本装置で IPv6 マルチキャスト通信障害が発生した場合の対処について説明します。

3.12.1 IPv6 PIM-SM ネットワークで通信ができない

IPv6 PIM-SM ネットワーク構成でマルチキャスト中継ができない場合は，以下に示す障害解析方法に従って原因の切り分けを行ってください。

IPv6 PIM-SM のネットワーク例を次の図に示します。

図 3-16 IPv6 PIM-SM ネットワーク例

注

- BSR：ランデブーポイントの情報を配信するルータ（詳細は，マニュアル「コンフィグレーションガイド」を参照してください）
- ランデブーポイントルータ：中継先が確定していないパケットをマルチキャスト受信者方向に中継するルータ（詳細は，マニュアル「コンフィグレーションガイド」を参照してください）
- first-hop-router：マルチキャスト送信者と直接接続するルータ
- last-hop-router：マルチキャスト受信者と直接接続するルータ

(1) 共通確認内容

次の表に，IPv6 PIM-SM ネットワーク構成のすべての本装置に対する共通確認内容を示します。

表 3-40 共通確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションにマルチキャスト機能を使用する指定（ipv6 multicast routing）があることを確認してください。 show running-config	マルチキャスト機能を使用する指定がない場合は，コンフィグレーションを修正してください。
2	コンフィグレーションに loopback インタフェースのアドレス設定があることを確認してください。 show running-config	loopback インタフェースのアドレス設定がない場合はコンフィグレーションを修正してください。
3	一つ以上のインタフェースで PIM が動作していることを確認してください。 show ipv6 pim interface	動作していない場合はコンフィグレーションを確認し，どれか一つ以上のインタフェースで PIM が動作するように設定してください。

項番	確認内容・コマンド	対応
4	PIM が動作するインタフェースに，MLD snooping が設定されているか確認してください。 show mld-snooping	MLD snooping が設定されている場合は，以下の内容を確認してください。 • 隣接ルータと接続しているポートに対して MLD snooping のマルチキャストルータポートの設定がされているか確認してください。 • 「3.6.5　MLD snooping によるマルチキャスト中継ができない」を参照してください。
5	PIM および MLD が動作するインタフェースで，フィルタなどによるプロトコルパケットおよびマルチキャストパケット中継を抑止する設定がないことを，コンフィグレーションで確認してください。 show running-config	プロトコルパケットおよびマルチキャストパケット中継を抑止する設定がある場合は，コンフィグレーションを修正してください。フィルタ設定情報の確認手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。
6	PIM の隣接情報を確認してください。 show ipv6 pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ipv6 pim コマンドで interface パラメータを指定して確認してください。 • 隣接ルータの設定を確認してください。
7	マルチキャストデータ送信者へのユニキャスト経路が存在するか確認してください。 show ipv6 route	ユニキャスト経路が存在しない場合は「3.11　IPv6 ユニキャストルーティングの通信障害」を参照してください。
8	マルチキャストデータ送信者への次ホップアドレスと接続しているインタフェースで，PIM が動作していることを確認してください。 show ipv6 pim interface	動作していない場合はコンフィグレーションを確認し，マルチキャストデータ送信者への次ホップアドレスと接続しているインタフェースで PIM が動作するように設定してください。
9	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていないことをコンフィグレーションで確認してください。 show running-config	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれている場合は，コンフィグレーションを修正してください。
10	BSR が決定されていることを確認してください。ただし，中継対象グループアドレスに対するランデブーポイントが静的ランデブーポイントの場合は，確認不要です。 show ipv6 pim bsr	BSR が決定されていない場合は BSR へのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「3.11　IPv6 ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，BSR の設定を確認してください。BSR が本装置の場合は，「(2) BSR 確認内容」を参照してください。
11	ランデブーポイントが決定されていることを確認してください。 show ipv6 pim rp-mapping	ランデブーポイントが決定されていない場合は，ランデブーポイントへのユニキャスト経路が存在するか確認してください。ユニキャスト経路が存在しない場合は，「3.11　IPv6 ユニキャストルーティングの通信障害」を参照してください。 ユニキャスト経路が存在する場合は，ランデブーポイントの設定を確認してください。ランデブーポイントが本装置の場合は，「(3) ランデブーポイントルータ確認内容」を参照してください。
12	ランデブーポイントのグループアドレスに中継対象グループアドレスが含まれていることを確認してください。 show ipv6 pim rp-mapping	中継対象グループアドレスが含まれていない場合は，ランデブーポイントルータの設定を確認してください。
13	マルチキャスト中継エントリが存在することを確認してください。 show ipv6 mcache	マルチキャスト中継エントリが存在しない場合は，上流ポートにマルチキャストデータが届いていることを確認してください。マルチキャストデータが届いていない場合は，マルチキャスト送信者あるいは上流ルータの設定を確認してください。

項番	確認内容・コマンド	対応
14	マルチキャスト経路情報が存在することを確認してください。 show ipv6 mroute	マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
15	マルチキャスト経路情報かマルチキャスト中継エントリが上限を超えていないか確認してください。 マルチキャスト経路情報： show ipv6 mroute マルチキャスト中継エントリ： show ipv6 mcache netstat multicast	Warning が出力されている場合は，想定していないマルチキャスト経路情報またはマルチキャスト中継エントリが作成されていないか確認してください。マルチキャスト中継エントリでネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。

(2) BSR 確認内容

次の表に，IPv6 PIM-SM ネットワーク構成で本装置が BSR の場合の確認内容を示します。

表 3-41 BSR 確認内容

項番	確認内容・コマンド	対応
1	本装置が BSR 候補であることを確認してください。 show ipv6 pim bsr	本装置が BSR 候補でない場合はコンフィグレーションを確認し，BSR 候補として動作するように設定してください。また，loopback インタフェースにアドレスが設定されていないと BSR 候補として動作しないため，loopback インタフェースにアドレスが設定されていることも確認してください。
2	本装置が BSR であることを確認してください。 show ipv6 pim bsr	本装置が BSR でない場合は，ほかの BSR 候補の優先度を確認してください。優先度は値の大きい方が高くなります。優先度が同じ場合は，BSR アドレスが一番大きい BSR 候補が BSR となります。

(3) ランデブーポイントルータ確認内容

次の表に，IPv6 PIM-SM ネットワーク構成で本装置がランデブーポイントルータの場合の確認内容を示します。

表 3-42 ランデブーポイントルータ確認内容

項番	確認内容・コマンド	対応
1	本装置が中継対象グループアドレスに対するランデブーポイント候補であることを確認してください。 show ipv6 pim rp-mapping	本装置が中継対象グループアドレスに対するランデブーポイント候補でない場合は，コンフィグレーションを確認し，中継対象グループアドレスに対するランデブーポイント候補として動作するように設定してください。また，loopback インタフェースにアドレスが設定されていないとランデブーポイント候補として動作しないため，loopback インタフェースにアドレスが設定されていることも確認してください。
2	本装置が中継対象グループアドレスに対するランデブーポイントであることを確認してください。 show ipv6 pim rp-hash <Group Address>	本装置がランデブーポイントでない場合は，ほかのランデブーポイント候補の優先度を確認してください。優先度は値の小さい方が高くなります。ほかのランデブーポイント候補の優先度が高い場合はランデブーポイントとして動作せず，優先度が同一の場合はプロトコルの仕様でグループアドレス単位に分散され，該当グループに対してランデブーポイントとして動作しないことがあります。本装置を優先的にランデブーポイントとして動作させる場合は，ほかのランデブーポイント候補より高い優先度を設定してください。

(4) last-hop-router 確認内容

次の表に，IPv6 PIM-SM ネットワーク構成で本装置が last-hop-router の場合の確認内容を示します。

表 3-43 last-hop-router 確認内容

項番	確認内容・コマンド	対応
1	マルチキャスト受信者と接続しているインタフェースで，MLD が動作していることを確認してください。 show ipv6 mld interface	動作していない場合はコンフィグレーションを確認し，MLD が動作するように設定してください。
2	マルチキャスト受信者が MLD で中継対象グループに参加していることを確認してください。 show ipv6 mld group	中継対象グループに参加していない場合は，マルチキャスト受信者の設定を確認してください。
3	中継対象グループが参加し，PIM が動作しているインタフェースがある場合は，本装置が DR であることを確認してください。 show ipv6 pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を調査してください。
4	静的グループ参加機能が動作するインタフェースに，MLD snooping が設定されているか確認してください。 show mld-snooping	MLD snooping が設定されている場合は，以下の内容を確認してください。 • 中継先ポートに対して MLD snooping のマルチキャストルータポートの設定がされているか確認してください。 • 「3.6.5 MLD snooping によるマルチキャスト中継ができない」を参照してください。
5	各インタフェースで異常を検出していないか確認してください。 show ipv6 mld interface	Notice を確認し，警告情報が出力されていないことを確認してください。 警告情報が出力されている場合は以下を確認してください。 • L：想定した最大数を超えて参加要求が発生しています。接続ユーザ数を確認してください。 • Q：隣接するルータと MLD のバージョンが不一致となっています。MLD のバージョンを合わせてください。 • R：現在の設定では受信できない Report を送信しているユーザが存在します。本装置の MLD のバージョンを変更するか，参加ユーザの設定を確認してください。 • S：MLDv2 で 1 メッセージ内に格納できるソース数が上限を超えたため参加情報を一部廃棄しています。参加ユーザの設定を確認してください。

(5) first-hop-router 確認内容

次の表に，IPv6 PIM-SM ネットワーク構成で本装置が first-hop-router の場合の確認内容を示します。

表 3-44 first-hop-router 確認内容

項番	確認内容・コマンド	対応
1	本装置がマルチキャスト送信者と直接接続していることを確認してください。	直接接続していない場合はネットワーク構成を確認してください。
2	マルチキャスト送信者と接続しているインタフェースで，PIM または MLD が動作していることを確認してください。 show ipv6 pim interface show ipv6 mld interface	動作していない場合はコンフィグレーションを確認し，PIM または MLD が動作するように設定してください。

項番	確認内容・コマンド	対応
3	マルチキャスト経路情報が存在するか確認してください。 show ipv6 mroute	マルチキャスト経路情報が存在しない場合は，マルチキャストデータ送信元アドレスが，マルチキャスト送信者と直接接続しているインタフェースのネットワークアドレスであることを確認してください。

3.12.2 IPv6 PIM-SM ネットワークでマルチキャストデータが二重中継される

IPv6 PIM-SM ネットワーク構成でマルチキャストデータが二重中継される場合は，各ルータの設定内容を確認し，同一ネットワークに複数のルータが存在するインタフェースでは PIM が動作するように設定してください。

上記の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 3-45 二重中継が継続する場合の確認内容

項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの，PIM の隣接情報を確認してください。 show ipv6 pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ipv6 pim コマンドで interface パラメータを指定して確認してください。 • フィルタなどによるプロトコルパケットの中継を抑止する設定がないことを，コンフィグレーションで確認してください。フィルタ設定情報の確認手順については，「3.22.1 フィルタ /QoS 設定情報の確認」を参照してください。 • 隣接ルータの設定を確認してください。

3.12.3 IPv6 PIM-SSM ネットワークで通信ができない

IPv6 PIM-SSM ネットワーク構成でマルチキャスト中継ができない場合は，以下に示す障害解析方法に従って原因の切り分けを行ってください。

IPv6 PIM-SSM のネットワーク例を次の図に示します。

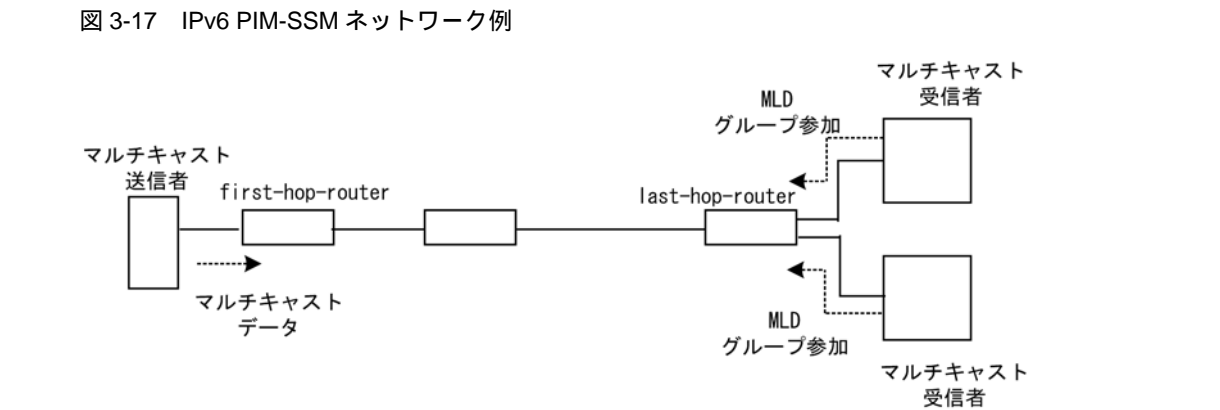



図 3-17 IPv6 PIM-SSM ネットワーク例

注

- first-hop-router：マルチキャスト送信者と直接接続するルータ
- last-hop-router：マルチキャスト受信者と直接接続するルータ

(1) 共通確認内容

次の表に，IPv6 PIM-SSM ネットワーク構成のすべての本装置に対する共通確認内容を示します。

表 3-46 共通確認内容

項番	確認内容・コマンド	対応
1	コンフィグレーションにマルチキャスト機能を使用する指定（ipv6 multicast routing）があることを確認してください。 show running-config	マルチキャスト機能を使用する指定がない場合は，コンフィグレーションを修正してください。
2	コンフィグレーションに loopback インタフェースのアドレス設定があることを確認してください。 show running-config	loopback インタフェースのアドレス設定がない場合はコンフィグレーションを修正してください。
3	一つ以上のインタフェースで PIM が動作していることを確認してください。 show ipv6 pim interface	動作していない場合はコンフィグレーションを確認し，どれか一つ以上のインタフェースで PIM が動作するように設定してください。
4	PIM が動作するインタフェースに，MLD snooping が設定されているか確認してください。 show mld-snooping	MLD snooping が設定されている場合は，以下の内容を確認してください。 • 隣接ルータと接続しているポートに対して MLD snooping のマルチキャストルータポートの設定がされているか確認してください。 • 「3.6.5　MLD snooping によるマルチキャスト中継ができない」を参照してください。
5	PIM および MLD が動作するインタフェースで，フィルタなどによるプロトコルパケットおよびマルチキャストパケット中継を抑止する設定がないことを，コンフィグレーションで確認してください。 show running-config	プロトコルパケットおよびマルチキャストパケット中継を抑止する設定がある場合は，コンフィグレーションを修正してください。フィルタ設定情報の確認手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。
6	PIM の隣接情報を確認してください。 show ipv6 pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ipv6 pim コマンドで interface パラメータを指定して確認してください。 • 隣接ルータの設定を確認してください。
7	マルチキャストデータ送信者へのユニキャスト経路が存在するか確認してください。 show ipv6 route	ユニキャスト経路が存在しない場合は「3.11　IPv6 ユニキャストルーティングの通信障害」を参照してください。
8	マルチキャストデータ送信者へのユニキャスト経路送出インタフェースで，PIM が動作していることを確認してください。 show ipv6 pim interface	動作していない場合はコンフィグレーションを確認し，ユニキャスト経路送出インタフェースで PIM が動作するように設定してください。
9	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていることを，コンフィグレーションで確認してください。 show running-config	PIM-SSM のグループアドレスに中継対象グループアドレスが含まれていない場合は，コンフィグレーションを修正してください。
10	マルチキャスト経路情報が存在するか確認してください。 show ipv6 mroute	マルチキャスト経路情報が存在しない場合は，下流ルータの設定を確認してください。
11	マルチキャスト経路情報かマルチキャスト中継エントリが上限を超えていないか確認してください。 マルチキャスト経路情報： show ipv6 mroute マルチキャスト中継エントリ： show ipv6 mcache netstat multicast	Warning が出力されている場合は，想定していないマルチキャスト経路情報またはマルチキャスト中継エントリが作成されていないか確認してください。マルチキャスト中継エントリでネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。

(2) last-hop-router 確認内容

次の表に，IPv6 PIM-SSM ネットワーク構成で本装置が last-hop-router の場合の確認内容を示します。

表 3-47 last-hop-router 確認内容

項番	確認内容・コマンド	対応
1	マルチキャスト受信者のモードが MLDv1/MLDv2（EXCLUDE モード）の場合は，コンフィグレーションに MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM が使用できる指定（ipv6 mld ssm-map enable）があることを確認してください。 show running-config	MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM が使用できる指定がない場合は，コンフィグレーションを修正してください。
2	マルチキャスト受信者のモードが MLDv1/MLDv2（EXCLUDE モード）の場合は，コンフィグレーションに PIM-SSM で中継するグループアドレスと送信元アドレスが，MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM と連携動作する設定（ipv6 mld ssm-map static）があることを確認してください。 show running-config	MLDv1/MLDv2（EXCLUDE モード）で PIM-SSM と連携動作する設定がない場合は，コンフィグレーションを修正してください。
3	マルチキャスト受信者と接続しているインタフェースで，MLD が動作していることを確認してください。 show ipv6 mld interface	動作していない場合はコンフィグレーションを確認し，MLD が動作するように設定してください。
4	マルチキャスト受信者と接続しているインタフェースで，MLD 警告情報が表示されていないことを確認してください。 show ipv6 mld interface	表示されている場合は，それぞれの警告にあった対応をしてください。警告の内容については，マニュアル「運用コマンドレファレンス」を参照してください。
5	マルチキャスト受信者が MLD で中継対象グループに参加していることを確認してください。 show ipv6 mld group	中継対象グループにグループ参加していない場合は，マルチキャスト受信者の設定を確認してください。
6	MLD グループ情報に送信元アドレスが登録されていることを確認してください。 show ipv6 mld group	マルチキャスト受信者のモードが MLDv2（INCLUDE モード）で送信元アドレスが登録されていない場合は，マルチキャスト受信者を調査してください。マルチキャスト受信者のモードが MLDv1/MLDv2（EXCLUDE モード）の場合は，PIM-SSM と連携動作する設定があることをコンフィグレーションで確認してください。
7	中継対象グループが参加し，PIM が動作しているインタフェースがある場合は，本装置が DR であることを確認してください。 show ipv6 pim interface	本装置が DR でない場合は，中継対象インタフェースの DR を調査してください。
8	静的グループ参加機能が動作するインタフェースに，MLD snooping が設定されているか確認してください。 show mld-snooping	MLD snooping が設定されている場合は，以下の内容を確認してください。 • 中継先ポートに対して MLD snooping のマルチキャストルータポートの設定がされているか確認してください。 • 「3.6.5　MLD snooping によるマルチキャスト中継ができない」を参照してください。

項番	確認内容・コマンド	対応
9	各インタフェースで異常を検出していないか確認してください。 show ipv6 mld interface	Notice を確認し，警告情報が出力されていないことを確認してください。 警告情報が出力されている場合は以下を確認してください。 • L：想定した最大数を超えて参加要求が発生しています。接続ユーザ数を確認してください。 • Q：隣接するルータと MLD のバージョンが不一致となっています。MLD のバージョンを合わせてください。 • R：現在の設定では受信できない Report を送信しているユーザが存在します。本装置の MLD のバージョンを変更するか，参加ユーザの設定を確認してください。 • S：MLDv2 で 1 メッセージ内に格納できるソース数が上限を超えたため参加情報を一部廃棄しています。参加ユーザの設定を確認してください。

(3) first-hop-router 確認内容

次の表に，IPv6 PIM-SSM ネットワーク構成で本装置が first-hop-router の場合の確認内容を示します。

表 3-48　first-hop-router 確認内容

項番	確認内容・コマンド	対応
1	本装置がマルチキャスト送信者と直接接続していることを確認してください。	直接接続していない場合は，ネットワーク構成を確認してください。
2	マルチキャスト送信者と接続しているインタフェースで，PIM または MLD が動作していることを確認してください。 show ipv6 pim interface show ipv6 mld interface	動作していない場合はコンフィグレーションを確認し，PIM または MLD が動作するように設定してください。
3	マルチキャストデータが本装置に届いているか確認してください。	マルチキャストデータが届いていない場合は，マルチキャスト送信者の設定を確認してください。
4	マルチキャストデータとマルチキャスト経路情報のグループアドレスと送信元アドレスが一致するか確認してください。 show ipv6 mroute show netstat multicast	グループアドレスと送信元アドレスが一致しない場合は，マルチキャスト送信者と last-hop-router の設定内容を確認してください。

3.12.4 IPv6 PIM-SSM ネットワークでマルチキャストデータが二重中継される

IPv6 PIM-SSM ネットワーク構成でマルチキャストデータが二重中継される場合は，各ルータの設定内容を確認し，同一ネットワークに複数のルータが存在するインタフェースでは PIM が動作するように設定してください。

上記の設定をしても二重中継が継続する場合の確認内容を次の表に示します。

表 3-49　二重中継が継続する場合の確認内容

項番	確認内容・コマンド	対応
1	同一ネットワークに複数のルータが存在するインタフェースの，PIM の隣接情報を確認してください。 show ipv6 pim neighbor	隣接ルータが表示されない場合は以下の内容を確認してください。 • 隣接ルータと接続しているインタフェースで PIM が動作していることを show ipv6 pim コマンドで interface パラメータを指定して確認してください。 • フィルタなどによるプロトコルパケットの中継を抑止する設定がないことを，コンフィグレーションで確認してください。フィルタ設定情報の確認手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。 • 隣接ルータの設定を確認してください。

3.12.5　VRF での IPv6 マルチキャスト通信のトラブル

VRF での IPv6 マルチキャスト通信のトラブルは，以下の確認を行ってください。

表 3-50　VRF での確認内容

項番	確認内容・コマンド	対応
1	VRF のインタフェースが正しいか，ポート番号および VLAN ID を確認してください。 show ipv6 vrf show vlan show ipv6 pim interface	正しくない場合はコンフィグレーションまたは接続を修正してください。
2	本装置がランデブーポイントの場合，該当 VRF で本装置がランデブーポイント候補として動作していることを確認してください。 show ipv6 pim vrf all rp-mapping	ランデブーポイント候補として動作していない場合は，コンフィグレーションのランデブーポイント候補の設定で，該当 VRF の loopback インタフェースのアドレスが指定されているか確認してください。 show running-config
3	本装置が BSR の場合，該当 VRF で本装置が BSR 候補として動作していることを確認してください。 show ipv6 pim vrf all bsr	BSR 候補として動作していない場合は，コンフィグレーションの BSR 候補の設定で，該当 VRF の loopback インタフェースのアドレスが指定されているか確認してください。 show running-config
4	複数の VRF で運用している場合，グローバルネットワークまたは特定の VRF がマルチキャスト中継エントリを想定以上に占有していないか確認してください。 show ipv6 mcache vrf all	ネットワーク設計の想定以上にマルチキャスト中継エントリを占有しているグローバルネットワークまたは VRF があった場合は，想定していないマルチキャスト中継エントリが作成されていないか確認してください。ネガティブキャッシュが多い場合は，不要なパケットを送信している端末が存在しないか確認してください。 また，VRF ごとの中継エントリの最大数を設定して一つのグローバルネットワークまたは特定の VRF が中継エントリを占有しないようにしてください。 該当するコンフィグレーション： ipv6 pim vrf <vrf id> mcache-limit <number>
5	各 VRF に対し，「3.12.1　IPv6 PIM-SM ネットワークで通信ができない」～「3.12.4　IPv6 PIM-SSM ネットワークでマルチキャストデータが二重中継される」の確認をしてください。	情報確認のための各コマンドは VRF を指定する必要があります。VRF 指定の方法は，マニュアル「運用コマンドレファレンス」を参照してください。

3.12.6　エクストラネットでの IPv6 マルチキャスト通信のトラブル

エクストラネットでの IPv6 マルチキャスト通信のトラブルは，まず，「3.12.5　VRF での IPv6 マルチキャスト通信のトラブル」を確認し，各 VRF でマルチキャスト通信ができることを確認してください。次に，以下の確認を行ってください。

表 3-51 エクストラネットでの確認内容

項番	確認内容・コマンド	対応
1	中継先 VRF から送信元のアドレスへのユニキャスト経路が，期待する VRF またはグローバルネットワークであることを確認してください。 show ipv6 rpf	正しくない場合はユニキャストエクストラネットの設定を見直してください。
2	エクストラネットで使用する IPv6 マルチキャストアドレスに対応するプロトコル（PIM-SM または PIM-SSM）が，中継先 VRF と上流側 VRF で同じであることを確認してください。 show running-config	プロトコルが異なる場合は，中継先 VRF と上流側 VRF で同じプロトコルとなる IPv6 マルチキャストアドレスを使用してください。
3	上流側 VRF で，送信元アドレスへのユニキャスト経路が，さらに別の VRF になっていないか確認してください。 show ipv6 rpf	上流側 VRF で，送信元アドレスへのユニキャスト経路がその VRF 内の実インタフェースである VRF となるようにしてください。
4	PIM-SM VRF ゲートウェイを使用する場合，上流側 VRF に (*,G) エントリが生成されていることを確認してください。また，該当する (*,G) エントリの表示項目 Flags に "V" が表示されていることを確認してください。 show ipv6 mroute	(*,G) エントリが正常に生成されていない場合，上流側 VRF の IPv6 マルチキャスト経路フィルタリングにエクストラネット通信で使用する IPv6 マルチキャストアドレスが，ホストアドレス指定で許可されていることを確認してください。
5	PIM-SM VRF ゲートウェイを使用する場合，上流側 VRF で生成された (*,G) エントリの下流インタフェースに中継先 VRF が表示されていることを確認してください。 show ipv6 mroute	上流側 VRF の (*,G) エントリの downstream に中継先 VRF が存在しない場合，上流側 VRF の IPv6 マルチキャスト経路フィルタリングのホストアドレス指定をしている route-map に，中継先 VRF が許可されていることを確認してください。 なお，route-map の match vrf による個別 VRF 指定がない場合は，すべての VRF が中継先として許可されています。
6	show ipv6 mroute で上流インタフェースの VRF 表示に "(denied)" が表示されている場合は，上流側 VRF の IPv6 マルチキャスト経路フィルタリングが正しく設定されていません。コンフィグレーションで上流側 VRF の IPv6 マルチキャスト経路フィルタリングを確認してください。 show ipv6 mroute show running-config	上流側 VRF の IPv6 マルチキャスト経路フィルタリングにエクストラネット通信で使用する IPv6 マルチキャストアドレスと中継先 VRF を許可していることを確認してください。 なお，IPv6 マルチキャスト経路フィルタリングに IPv6 マルチキャストアドレスおよび VRF が個別指定されていない場合は，IPv6 マルチキャストアドレスおよび VRF のすべてが許可されています。

3.13　レイヤ 2 認証の通信障害

3.13.1　IEEE 802.1X 使用時の通信障害

IEEE 802.1X 使用時に認証ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-52　IEEE 802.1X の認証障害解析方法

項番	確認内容・コマンド	対応
1	show dot1x コマンドを実行し，IEEE802.1X の動作状態を確認してください。	「Dot1x doesn't seem to be running」が表示された場合は，IEEE802.1X が停止しています。dot1x system-auth-control コマンドが設定されているかコンフィグレーションを確認してください。 「System 802.1X : Enable」が表示された場合は項番 2 へ。
2	show dot1x statistics コマンドを実行し，EAPOL のやりとりが行われていることを確認してください。	[EAPOL frames] の RxTotal が 0 の場合は端末から EAPOL が送信されていません。また，RxInvalid または RxLenErr が 0 でない場合は端末から不正な EAPOL を受信しています。不正な EAPOL を受信した場合はログを採取します。ログは show dotlx logging コマンドで閲覧できます。また，ログは「Invalid EAPOL frame received」メッセージと共に不正な EAPOL の内容となります。上記に該当する場合は端末の Supplicant の設定を確認してください。 上記に該当しない場合は項番 3 へ。
3	show dot1x statistics コマンドを実行し，RADIUS サーバへの送信が行われていることを確認してください。	[EAP overRADIUS frames] の TxNoNakRsp が 0 の場合は RADIUS サーバへの送信が行われていません。以下について確認してください。 • コンフィグレーションコマンドで aaa authentication dot1x default group radius が設定されているか確認してください。 • コンフィグレーションコマンド radius-server host が正しく設定されているか確認してください。 • 認証モードがポート単位認証および VLAN 単位認証（静的）の場合，認証端末がコンフィグレーションコマンド mac-address-table static で登録されていないことを確認してください。VLAN 単位認証（動的）では，コンフィグレーションコマンド mac-address で登録されていないことを確認してください。 • 認証モードが VLAN 単位認証（動的）の場合は，コンフィグレーションコマンドで aaa authorization network default group radius が設定されているか確認してください。 上記に該当しない場合は項番 4 へ。
4	show dot1x statistics コマンドを実行し，RADIUS サーバからの受信が行われていることを確認してください。	[EAP overRADIUS frames] の RxTotal が 0 の場合は RADIUS サーバからのパケットを受信していません。以下について確認してください。 • RADIUS サーバがリモートネットワークに収容されている場合はリモートネットワークへの経路が存在することを確認してください。 • RADIUS サーバのポートが認証対象外となっていることを確認してください。 上記に該当しない場合は項番 5 へ。
5	show dot1x logging コマンドを実行し，RADIUS サーバとのやりとりを確認してください。	• 「Invalid EAP over RADIUS frames received」がある場合 RADIUS サーバから不正なパケットを受信しています。RADIUS サーバが正常に動作しているか確認してください。 • 「Failed to connect to RADIUS server」がある場合，RADIUS サーバへの接続が失敗しています。RADIUS サーバが正常に動作しているか確認してください。 上記に該当しない場合は項番 6 へ。

項番	確認内容・コマンド	対応
6	show dot1x logging コマンドを実行し，認証が失敗していないか確認してください。	• 「New Supplicant Auth Fail.」がある場合，以下の要因で認証が失敗しています。問題ないか確認してください。 (1) ユーザ ID またはパスワードが，認証サーバに登録されていない。 (2) ユーザ ID またはパスワードの入力ミス。 • 「The number of supplicants on the switch is full」がある場合，装置の最大 supplicant 数を超えたため，認証が失敗しています。 • 「The number of supplicants on the interface is full」がある場合，インタフェース上の最大 supplicant 数を超えたため，認証が失敗しています。 • 「Failed to authenticate the supplicant because it could not be registered to mac-address-table.」がある場合，認証は成功したが，H/W の MAC アドレステーブル設定に失敗しています。マニュアル「メッセージ・ログレファレンス」の該当個所を参照し，記載されている［対応］に従って対応してください。 • 「Failed to authenticate the supplicant because it could not be registered to MAC VLAN.」がある場合，認証は成功したが，H/W の MAC VLAN テーブル設定に失敗しています。 マニュアル「メッセージ・ログレファレンス」の該当個所を参照し，記載されている［対応］に従って対応してください。 上記に該当しないで，認証対象ポートが VLAN 単位認証（動的）である場合は項番 7 へ。 それ以外の認証単位の場合は，RADIUS サーバのログを参照して認証が失敗していないか確認してください。

項番	確認内容・コマンド	対応
7	show dot1x logging コマンドを実行し，VLAN 単位認証（動的）の動的割り当てが失敗していないか確認してください。	• 「Failed to assign VLAN.(Reason: No Tunnel-Type Attribute)」がある場合，RADIUS フレームの RADIUS 属性に Tunnel-Type 属性がないため，動的割り当てに失敗しています。RADIUS サーバの RADIUS 属性の設定で Tunnel-Type 属性を追加設定してください。 • 「Failed to assign VLAN.(Reason:Tunnel-Type Attribute is not VLAN(13))」がある場合，RADIUS 属性の Tunnel-Type 属性の値が VLAN(13) でないため，動的割り当てに失敗しています。RADIUS サーバに設定する Tunnel-Type 属性の値を VLAN(13) に設定してください。 • 「Failed to assign VLAN.(Reason: No Tunnel-Medium-Type Attribute)」がある場合，RADIUS 属性の Tunnel-Medium-Type 属性がないため，動的割り当てに失敗しています。RADIUS サーバの RADIUS 属性 Tunnel-Medium-Type 属性を追加設定してください。 • 「Failed to assign VLAN. (Reason: Tunnel-Medium-Type Attribute is not IEEE802(6))」がある場合，Tunnel-Medium-Type 属性の値が IEEE802(6) でないか，または Tunnel-Medium-Type の値は一致しているが Tag 値が Tunnel-Type 属性の Tag が一致していないため動的割り当てに失敗しています。RADIUS サーバの RADIUS 属性の Tunnel-Medium-Type 属性の値または Tag を正しい値に設定してください。 • 「Failed to assign VLAN. (Reason: No Tunnel-Private-Group-ID Attribute)」がある場合，RADIUS サーバの RADIUS 属性である Tunnel-Private-Group-ID 属性が設定されていないため，動的割り当てに失敗しています。RADIUS サーバの RADIUS 属性の Tunnel-Private-Group-ID 属性の設定をしてください。 • 「Failed to assign VLAN. (Reason: Invalid Tunnel-Private-Group-ID Attribute)」がある場合，RADIUS 属性の Tunnel-Private-Group-ID 属性に不正な値が入っているため，動的割り当てに失敗しています。RADIUS サーバの RADIUS 属性の Tunnel-Private-Group-ID 属性に正しい VLAN ID を設定してください。 • 「Failed to assign VLAN. (Reason: The VLAN ID is out of range.)」の場合がある場合，RADIUS サーバに設定した RADIUS 属性の Tunnel-Private-Group-ID 属性に設定した VLAN ID が範囲外のため，動的割り当てに失敗しています。Tunnel-Private-Group-ID 属性に正しい VLAN ID を設定してください。 • 「Failed to assign VLAN. (Reason: The port doesn't belong to VLAN.)」がある場合，認証ポートが RADIUS サーバの RADIUS 属性である Tunnel-Private-Group-ID 属性に指定された VLAN ID に属していないため，動的割り当てに失敗しています。RADIUS サーバの RADIUS 属性である Tunnel-Private-Group-ID 属性に設定された VLAN ID と認証ポートに設定された MAC VLAN の VLAN ID が一致するように設定してください。 • 「Failed to assign VLAN. (Reason: The VLAN ID is not set to radius-vlan.)」がある場合，RADIUS サーバの RADIUS 属性である Tunnel-Private-Group-ID 属性に指定された VLAN ID が VLAN 単位認証 (動的) の認証対象外の VLAN ID です。RADIUS サーバの RADIUS 属性である Tunnel-Private-Group-ID 属性に設定された VLAN ID と認証ポートに設定された MAC VLAN の VLAN ID が一致するように設定してください。 上記に該当しない場合は，RADIUS サーバのログを参照して認証が失敗していないか確認してください。

IEEE802.1X が動作するポートまたは VLAN で通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。該当しない場合は，「3.6　レイヤ 2 ネットワークの通信障害」を参照してください。

表 3-53 IEEE 802.1X の通信障害解析方法

項番	確認内容・コマンド	対応
1	トランクポートに VLAN 単位認証（静的）を設定した VLAN とそれ以外の VLAN が設定されていないことを確認してください。	VLAN 単位認証（静的）を設定した VLAN 以外での通信ができないため，認証除外ポートに設定するか，VLAN 単位認証（静的）を設定した VLAN とそれ以外の VLAN を異なるポートに設定してください。
2	認証済み端末が，同一 VLAN 内の非認証ポートに移動していないか確認してください。	本装置で認証している端末が，非認証ポートに移動した場合，認証情報が解除されないと通信ができません。clear dot1x auth-state コマンドを使用して，対象端末の認証状態を解除してください。

3.13.2 Web 認証使用時の通信障害

Web 認証使用時の障害については，「表 3-54 Web 認証の障害解析方法」に示す障害解析に従って原因を切り分けてください。

また，Web 認証のコンフィグレーションに関する確認，およびアカウンティングに関する確認についてはそれぞれ「表 3-55 Web 認証のコンフィグレーションの確認」，「表 3-56 Web 認証のアカウンティングの確認」に従って原因を切り分けてください。

表 3-54 Web 認証の障害解析方法

項番	確認内容・コマンド	対応
1	端末にログイン画面が表示されるかを確認してください。	• ログイン画面とログアウト画面が表示されない場合は項番 2 へ。 • ローカル認証方式でログイン画面が表示される場合は項番 5 へ。 • RADIUS 認証方式でログイン画面が表示される場合は項番 7 へ。 • 運用ログメッセージが表示される場合は項番 14 へ。
2	ログイン，ログアウトの URL が合っているかを確認してください。	• ログイン，ログアウトの URL が違っている場合は，正しい URL を使用してください。 • 固定 VLAN モード時およびダイナミック VLAN モード時で，ログイン画面，ログアウト画面が表示されない場合は，次の設定を確認し，正しく設定してください。 • Web 認証専用 IP アドレスがコンフィグレーションコマンド web-authentication ip address で設定されているか，または URL リダイレクトがコンフィグレーションコマンド web-authentication redirect enable で有効となっているかを確認してください。 • 上記に該当しない場合は項番 3 へ。

項番	確認内容・コマンド	対応
3	Web サーバが動作しているかを確認してください。	• 次のコマンドを実行して Web サーバが動作しているかを確認します。Web サーバが動作している場合は項番 4 へ。 [コマンド] `# ps -auwx | grep httpd` [確認手順] ps コマンドの表示結果に /usr/local/sbin/httpd の表示があれば，Web サーバが動作しています。 • Web サーバが動作していない場合は，コンフィグレーションコマンド web-authentication web-port を確認してください。 • Web 認証のコンフィグレーションコマンドが正しく設定されている場合は，restart web-authentication web-server コマンドで Web サーバを再起動してください。 • 上記の操作でも Web サーバが起動しない場合は，コンフィグレーションコマンド no web-authentication system-auth-control で Web 認証を停止させ，10 秒程度経過後にコンフィグレーションコマンド web-authentication system-auth-control で Web 認証を起動してください。
4	認証専用 IPv4 アクセスリストの設定を確認してください。	• 認証前状態の端末から装置外に特定のパケット通信を行う場合，認証専用 IPv4 アクセスリストが設定されていることを確認してください。 また，通常のアクセスリストと認証専用 IPv4 アクセスリストの両方を設定した場合，認証専用 IPv4 アクセスリストに設定したフィルタ条件が通常のアクセスリストにも設定されていることを確認してください。 • 通常のアクセスリストおよび認証専用 IPv4 アクセスリストに，IP パケットを廃棄するフィルタ条件（deny ip など）が設定されていないことを確認してください。 • 認証専用 IPv4 アクセスリストのフィルタ条件に，Web 認証専用 IP アドレスが含まれるアドレスが設定されていないことを確認してください。 • 認証専用 IPv4 アクセスリストのフィルタ条件の宛先 IP アドレスに，any が指定されていないことを確認してください。 • 上記に該当しない場合は項番 9 へ。
5	show web-authentication user コマンドでユーザ ID が登録されているかを確認してください。	• ユーザ ID が登録されていない場合は，set web-authentication user コマンドでユーザ ID，パスワード，および VLAN ID を登録してください。 • 上記に該当しない場合は項番 6 へ。
6	入力したパスワードが合っているかを確認してください。	• パスワードが一致していない場合は，set web-authentication passwd コマンドでパスワードを変更するか，remove web-authentication user コマンドでユーザ ID をいったん削除したあとに，set web-authentication user コマンドで，再度，ユーザ ID，パスワード，および VLAN ID を登録してください。 • 上記に該当しない場合は項番 9 へ。

項番	確認内容・コマンド	対応
7	show web-authentication statistics コマンドで RADIUS サーバとの通信状態を確認してください。	• 表示項目 "[RADIUS frames]" の "TxTotal" の値が "0" の場合は，コンフィグレーションコマンドの aaa authentication web-authentication default group radius および radius-server host が正しく設定されているか確認してください。 • dead interval 機能によって，RADIUS サーバが無応答となった状態から通信可能な状態に復旧しても，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間の間は RADIUS サーバへの照合は行われないため，認証エラーとなります。 この際，RADIUS サーバ無応答による認証失敗の時間が長すぎる場合は，コンフィグレーションコマンド authentication radius-server dead-interval の設定値を変更するか，または clear web-authentication dead-interval-timer コマンドを実行してください。1 台目の RADIUS サーバを使用した認証動作が再開されます。 • 上記に該当しない場合は項番 8 へ。
8	RADIUS サーバにユーザ ID およびパスワードが登録されているかを確認してください。	• ユーザ ID が登録されていない場合は，RADIUS サーバに登録してください。 • 上記に該当しない場合は項番 9 へ。
9	show web-authentication statistics コマンドで Web 認証の統計情報が表示されるかを確認してください。	• Web 認証の統計情報が表示されない場合は項番 10 へ。 • 上記に該当しない場合は項番 11 へ。
10	コンフィグレーションコマンド web-authentication system-auth-control が設定されているかを確認してください。	• コンフィグレーションコマンド web-authentication system-auth-control が設定されていない場合は，設定してください。 • 上記に該当しない場合は項番 11 へ。
11	show web-authentication logging コマンドを実行し，動作に問題がないかを確認してください。	• 固定 VLAN モード時で，認証端末が接続されているポートの認証情報が表示されない場合は，コンフィグレーションコマンド web-authentication port で認証対象ポートが正しく設定されているかを確認してください。 また，端末が接続されている認証対象ポートがリンクダウンまたはシャットダウンしていないことを確認してください。 • 上記に該当しない場合は項番 13 へ。
12	アカウンティングサーバにアカウントが記録されない場合は，show web-authentication statistics コマンドでアカウンティングサーバとの通信状態を確認してください。	• 表示項目 "[Account frames]" の "TxTotal" の値が "0" の場合は，コンフィグレーションコマンドの aaa accounting web-authentication default start-stop group radius および radius-server host が正しく設定されているか確認してください。 • 上記に該当しない場合は Web 認証のコンフィグレーションを確認してください。
13	接続されている端末で認証ができない状態か確認してください。	• 認証対象端末の認証がまったくできない場合は，restart web-authentication web-server コマンドで Web サーバを再起動してください。 • Web サーバを再起動しても認証ができない場合は，restart vlan mac-manager コマンドを実行してください。 • 上記に該当しない場合は，Web 認証のコンフィグレーションを確認し，正しいコンフィグレーションを設定してください。

項番	確認内容・コマンド	対応
14	運用ログを show logging コマンドで確認してください。	• 次の操作が行われた場合，運用ログに Web サーバ (httpd) の停止メッセージと Web サーバ (httpd) の再起動メッセージが表示されることがあります。 (1)　Web 認証を停止 (no web-authentication system-auth-control コマンドの実行) した直後に，Web 認証を起動 (web-authentication system-auth-control コマンドの実行) した場合 (3)　restart web-authentication web-server コマンドで Web サーバを再起動した場合 [Web サーバ (httpd) の停止メッセージ] レベル：E7 メッセージ識別子：2a001000 メッセージ：httpd aborted. [Web サーバ (httpd) の再起動メッセージ] レベル：R7 メッセージ識別子：2a001000 メッセージ：httpd restarted. これは，Web サーバ (httpd) が停止して，その後，Web サーバ (httpd) が自動的に再起動したことを示します。Web サーバ (httpd) の再起動後は認証動作を継続できます。 • 上記に該当しない場合は，マニュアル「メッセージ・ログレファレンス」を参照してください。

Web 認証に関係するコンフィグレーションは次の点を確認してください。

表 3-55　Web 認証のコンフィグレーションの確認

項番	確認ポイント	確認内容
1	Web 認証のコンフィグレーション設定	次のコンフィグレーションコマンドが正しく設定されていることを確認してください。 ＜共通の設定＞ • aaa accounting web-authentication default start-stop group radius • aaa authentication web-authentication default group radius • web-authentication system-auth-control ＜ダイナミック VLAN モード時の設定＞ • web-authentication auto-logout • web-authentication max-timer • web-authentication max-user • web-authentication vlan ＜固定 VLAN モード時の設定＞ • web-authentication ip address • web-authentication port • web-authentication static-vlan max-user • web-authentication web-port • authentication arp-relay • authentication ip access-group • web-authentication redirect enable • web-authentication redirect-mode
2	VLAN インタフェースの IP アドレス設定	ダイナミック VLAN モード時，次の各 VLAN インタフェースに IP アドレスが正しく設定されていることを確認してください。 • 認証前 VLAN • 認証後 VLAN

項番	確認ポイント	確認内容
3	DHCP リレーエージェントの設定	ダイナミック VLAN モード時，L3 スイッチで外部 DHCP サーバを使用する場合，次の VLAN 間の DHCP リレーエージェントが正しく設定されていることを確認してください。 • 認証前 VLAN からサーバ用 VLAN 間 • 認証後 VLAN からサーバ用 VLAN 間
4	フィルタ設定	ダイナミック VLAN モード時，L3 スイッチで使用する場合，次の VLAN 間のフィルタが正しく設定されていることを確認してください。 • 認証用 VLAN から認証後 VLAN：全 IP 通信ができないように設定 • 認証後 VLAN から認証用 VLAN：Web ブラウザの通信だけ中継するように設定 なお，フィルタによって特定のパケットが廃棄されているか，または QoS 制御の帯域監視，廃棄制御もしくはシェーパによってパケットが廃棄されている可能性があります。コンフィグレーションのフィルタおよび QoS 制御の設定条件が正しいか，システム構築での帯域監視，廃棄制御またはシェーパのシステム運用が適切であるかを確認してください。手順については，「3.22.1　フィルタ /QoS 設定情報の確認」を参照してください。
5	認証用アクセスフィルタの設定を確認	固定 VLAN モード時およびダイナミック VLAN モード時，認証前状態の端末から装置外に通信するために必要なフィルタ条件が，コンフィグレーションコマンド authentication ip access-group および ip access-list extended で正しく設定されていることを確認してください。
6	ARP リレー設定を確認	固定 VLAN モード時およびダイナミック VLAN モード時，認証前状態の端末から本装置外の機器宛に ARP パケットを通信させるためのコンフィグレーションコマンド authentication arp-relay が正しく設定されているかを確認してください。

Web 認証のアカウンティングに関しては次の点を確認してください。

表 3-56　Web 認証のアカウンティングの確認

項番	確認ポイント	確認内容
1	認証結果のアカウントが正しく記録されているかの確認	• show web-authentication login コマンドを実行した際に認証状態が表示されていない場合は「表 3-54　Web 認証の障害解析方法」を実施してください。 • アカウンティングサーバに記録されていない場合は項番 2 へ。 • syslog サーバに記録されていない場合は項番 3 へ。
2	show web-authentication statistics コマンドでのアカウンティングサーバとの通信状態の確認	• 表示項目 "[Account frames]" の "TxTotal" の値が "0" の場合は，コンフィグレーションコマンド aaa accounting web-authentication default start-stop group radius，または radius-server host が正しく設定されているか確認してください。 • 上記に該当しない場合は，Web 認証のコンフィグレーションを確認してください。
3	syslog サーバの設定の確認	次のコンフィグレーションコマンドが正しく設定されていることを確認してください。 • logging host で syslog サーバが設定されていることを確認してください。 • logging event-kind でイベント種別に aut が設定されていることを確認してください。 • web-authentication logging enable が設定されていることを確認してください。

3.13.3　MAC 認証使用時の通信障害

MAC 認証使用時の障害については，「表 3-57　MAC 認証の障害解析方法」に示す障害解析に従って原因を切り分けてください。

また，MAC 認証のコンフィグレーションに関する確認，およびアカウンティングに関する確認についてはそれぞれ「表 3-58　MAC 認証のコンフィグレーションの確認」，「表 3-59　MAC 認証のアカウンティングの確認」に従って原因を切り分けてください。

表 3-57　MAC 認証の障害解析方法

項番	確認内容・コマンド	対応
1	端末が通信できるかを確認してください。	• ローカル認証方式で認証できない場合は項番 2 へ。 • RADIUS 認証方式で認証できない場合は項番 3 へ。 • 上記に該当しない場合は項番 5 へ。
2	show mac-authentication mac-address コマンドで MAC アドレスと VLAN ID が登録されているかを確認してください。	• MAC アドレスが登録されていない場合は，set mac-authentication mac-address コマンドで MAC アドレス，および VLAN ID を登録してください。 • 上記に該当しない場合は項番 5 へ。
3	show mac-authentication statistics コマンドで RADIUS サーバとの通信状態を確認してください。	• 表示項目 "[RADIUS frames]" の "TxTotal" の値が "0" の場合は，コンフィグレーションコマンド aaa authentication mac-authentication default group radius，radius-server host および mac-authentication radius-server host が正しく設定されているか確認してください。 • dead interval 機能によって，RADIUS サーバが無応答となった状態から通信可能な状態に復旧しても，コンフィグレーションコマンド authentication radius-server dead-interval で設定された時間の間は RADIUS サーバへの照合は行われないため，認証エラーとなります。 この際，RADIUS サーバ無応答による認証失敗の時間が長すぎる場合は，コンフィグレーションコマンド authentication radius-server dead-interval の設定値を変更するか，または clear mac-authentication dead-interval-timer コマンドを実行してください。1 台目の RADIUS サーバを使用した認証動作が再開されます。 • 上記に該当しない場合は項番 4 へ。
4	RADIUS サーバに MAC アドレスおよびパスワードが登録されているかを確認してください。	• RADIUS サーバのユーザ ID として MAC アドレスが登録されていない場合は，RADIUS サーバに登録してください。 • パスワードとして MAC アドレスを使用している場合は，ユーザ ID に設定した MAC アドレスと同一の値を設定してください。 • パスワードとして，RADIUS サーバに共通の値を設定した場合は，コンフィグレーションコマンド mac-authentication password で設定したパスワードと一致しているかを確認してください。 • 上記に該当しない場合は項番 5 へ。

項番	確認内容・コマンド	対応
5	認証専用 IPv4 アクセスリストの設定を確認してください。	• 認証前状態の端末から装置外に特定のパケット通信を行う場合，認証専用 IPv4 アクセスリストが設定されていることを確認してください。 また，通常のアクセスリストと認証専用 IPv4 アクセスリストの両方を設定した場合，認証専用 IPv4 アクセスリストに設定したフィルタ条件が通常のアクセスリストにも設定されていることを確認してください。 • 認証せずに通信できてしまう場合は，アクセスリストに，IP パケットの通信を許可するフィルタ条件（permit ip any など）が設定されていないことを確認してください。 • 認証対象ポートに設定した認証専用 IPv4 アクセスリストに deny ip any any のフィルタ条件を設定しても，受信した ARP パケットによって MAC 認証が行われます。該当ポートを MAC 認証の対象から外したい場合は，コンフィグレーションコマンド no mac-authentication port で MAC 認証の対象ポートから外してください。 • 上記に該当しない場合は項番 6 へ。
6	show mac-authentication statistics コマンドで MAC 認証の統計情報が表示されるかを確認してください。	• MAC 認証の統計情報が表示されない場合は項番 7 へ。 • 上記に該当しない場合は項番 8 へ。
7	コンフィグレーションコマンド mac-authentication system-auth-control が設定されているかを確認してください。	• コンフィグレーションコマンド mac-authentication system-auth-control が設定されていない場合は，設定してください。 • コンフィグレーションコマンド mac-authentication port で認証対象ポートが正しく設定されているかを確認してください。 • 端末が接続されている認証対象ポートがリンクダウン，またはシャットダウンしていないことを確認してください。 • 上記に該当しない場合は項番 8 へ。
8	show mac-authentication logging コマンドを実行し，動作に問題がないかを確認してください。	• 最大収容条件まで認証されている場合はほかの端末が認証解除するまでお待ちください。 • 上記に該当しない場合は MAC 認証のコンフィグレーションを確認してください。

MAC 認証に関係するコンフィグレーションは次の点を確認してください。

表 3-58　MAC 認証のコンフィグレーションの確認

項番	確認ポイント	確認内容
1	MAC 認証のコンフィグレーション設定	次のコンフィグレーションコマンドが正しく設定されていることを確認してください。 • aaa accounting mac-authentication default start-stop group radius • aaa authentication mac-authentication default group radius • mac-authentication password • mac-authentication port • mac-authentication radius-server host • mac-authentication static-vlan max-user • mac-authentication system-auth-control
2	認証用アクセスフィルタの設定を確認	認証前状態の端末から装置外に通信するために必要なフィルタ条件が，コンフィグレーションコマンド authentication ip access-group および ip access-list extended で，正しく設定されていることを確認してください。

MAC 認証のアカウンティングに関しては次の点を確認してください。

表 3-59 MAC 認証のアカウンティングの確認

項番	確認ポイント	確認内容
1	認証結果のアカウントが正しく記録されているかの確認	• show mac-authentication login に認証状態が表示されていない場合は「表 3-57 MAC 認証の障害解析方法」を実施してください。 • アカウンティングサーバに記録されていない場合は項番 2 へ。 • syslog サーバに記録されていない場合は項番 3 へ。
2	show mac-authentication statistics コマンドでのアカウンティングサーバとの通信状態の確認	• 表示項目 "[Account frames]" の "TxTotal" の値が "0" の場合は，コンフィグレーションコマンド aaa accounting mac-authentication default start-stop group radius, radius-server host，または mac-authentication radius-server host が正しく設定されているか確認してください。 • 上記に該当しない場合は MAC 認証のコンフィグレーションを確認してください。
3	syslog サーバの設定の確認	次のコンフィグレーションコマンドが正しく設定されていることを確認してください。 • logging host で syslog サーバが設定されていることを確認してください。 • logging event-kind でイベント種別に aut が設定されていることを確認してください。 • mac-authentication logging enable が設定されていることを確認してください。

3.14　高信頼性機能の通信障害

3.14.1　GSRP の通信障害

GSRP 構成で通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-60　GSRP 構成での通信障害時の解析方法

項番	確認内容・コマンド	対応
1	同一 GSRP グループを構成する本装置と相手装置で，通信障害となっている VLAN が所属する VLAN グループの状態を show gsrp コマンドで確認してください。	一方が Master，他方が Master 以外となっている場合は，項番 2 へ。
		一方が Backup(No Neighbor) となっている場合は，ダイレクトリンク間の通信異常を復旧してください。また，フィルタによって GSRP Advertise フレームが廃棄されているか，または QoS 制御の帯域監視，廃棄制御もしくはシェーパによって GSRP Advertise フレームが廃棄されている可能性があります。「3.22.1　フィルタ /QoS 設定情報の確認」を参照し，確認してください。 必要に応じ，Backup(No Neighbor) となっている一方を set gsrp master コマンドで Master にしてください。
		両方が Backup，または Backup(Waiting) となっている場合は，装置間でマスタ／バックアップ選択方法（Selection-Pattern）が同一となっているか確認してください。
		両方が Backup(Lock) となっている場合は，一方または両方のロック状態を解除してください。
		両方が Master となっている場合には，片方の GSRP プログラムを restart gsrp コマンドで再起動してください。
		その他の場合は，一時的な状態遷移の過渡状態です。しばらく通信復旧をお待ちください。
2	本装置の該当 VLAN ポートの状態，および通信パス上の装置を確認してください。	異常となっている本装置の該当 VLAN ポート，または通信パス上の装置を復旧してください。
		以下の条件をすべて満たす場合は，activate コマンドで該当 VLAN ポートを active 状態にしてください。 • 該当 VLAN ポートに対する MAC アドレステーブルフラッシュ方法が Reset である場合（show gsrp コマンドで port パラメータを指定して確認してください）
		本装置の該当 VLAN ポート，または通信パス上の装置に異常がない場合は項番 3 へ。
3	本装置の該当 VLAN ポートに対する MAC アドレステーブルフラッシュ方法（GSRP ／ Reset ／ No）を show gsrp コマンドで port パラメータを指定して確認してください。	MAC アドレステーブルフラッシュ方法が GSRP ／ Reset のどちらかであり，構成と合っていない場合は，コンフィグレーションコマンド gsrp reset-flush-port，gsrp no-flush-port を修正してください。
		MAC アドレステーブルフラッシュ方法が GSRP ／ Reset のどちらかであり，構成と合っている場合は，本装置の GSRP プログラムを restart gsrp コマンドで再起動してください。
		MAC アドレステーブルフラッシュ方法が No の場合は，通信パス上の隣接装置の MAC アドレステーブルがエージングされるまでお待ちください。

GSRP 構成でマスタ／バックアップが意図したとおりに切り替わらない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-61　GSRP 構成での状態異常時の障害解析方法

項番	確認内容・コマンド	対応
1	マスタ／バックアップが意図したとおりに切り替らない VLAN グループの状態を show gsrp コマンドで確認してください。	一方が Master，他方が Master 以外となっている場合は，項番 2 へ。
		一方が Backup(No Neighbor) となっている場合は，ダイレクトリンク間の通信異常を復旧してください。また，必要に応じ，Backup(No Neighbor) となっている一方を set gsrp master コマンドで Master にしてください。
		両方が Backup，または Backup(Waiting) となっている場合は，装置間でマスタ／バックアップ選択方法（Selection-Pattern）が同一となっているか確認してください。
		両方が Backup(Lock) となっている場合は，一方または両方のロック状態を解除してください。
		両方が Master となっている場合には，片方の GSRP プログラムを restart gsrp コマンドで再起動してください。
		その他の場合は，一時的な状態遷移の過渡状態です。しばらくお待ちください。
2	マスタ／バックアップ選択方法（Selection-Pattern）と本装置，および相手装置のアクティブポート数（Active-Ports），優先度情報（Priority），MAC アドレスに基づくマスタ／バックアップ選択が正しいかを show gsrp，show gsrp <GSRP-ID> vlan-group <VLAN group ID list> コマンドで確認してください。	正しいが，アクティブポート数（Active Ports）とアップポート数（Up Ports）が一致していない場合は，項番 3 へ。
		正しくない場合は，本装置の GSRP プログラムを restart gsrp コマンドで再起動してください。
3	アクティブポートに反映するまでの遅延時間（port-up-delay）と遅延残時間（delay）を show gsrp detail，show gsrp <GSRP-ID> port <Port list> コマンドで確認してください。	遅延時間（port-up-delay）が無限（infinity）であり，アップポート数（UP Ports）をアクティブポート数（Active Ports）に反映したい場合は，clear gsrp port-up-delay コマンドを実行してください。
		遅延時間（port-up-delay）が無限（infinity）でなく，遅延残時間（delay）が残っている場合は，遅延残時間後に反映されるため，お待ちください。また，即時に反映したい場合は，clear gsrp port-up-delay コマンドを実行してください。

GSRP 構成で GSRP Advertise フレームの受信タイムアウトを検出し，隣接不明状態になる場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-62　GSRP 構成での隣接不明時の障害解析方法

項番	確認内容・コマンド	対応
1	GSRP Advertise フレームの送信間隔（Advertise Interval），および GSRP Advertise フレームの保持時間（Advertise Hold Time）を show gsrp detail コマンドで確認してください。	GSRP Advertise フレームの保持時間が GSRP Advertise フレームの送信間隔より小さいか，または同じ場合は，GSRP Advertise フレームの保持時間に GSRP Advertise フレームの送信間隔より大きな値を設定してください。
		GSRP Advertise フレームの保持時間が GSRP Advertise フレームの送信間隔より大きい場合は，ネットワーク環境に応じて，GSRP Advertise フレームの保持時間を現在より大きい値に設定してください。
		「3.22.1　フィルタ /QoS 設定情報の確認」を参照し，フィルタ，QoS 制御の帯域監視，廃棄制御，またはシェーパによって GSRP Advertise フレームが廃棄される要因がないかを確認してください。

3.14.2 IPv4 ネットワークの VRRP 構成で通信ができない

VRRP 構成で通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-63 VRRP の障害解析方法

項番	確認内容・コマンド	対応
1	同一仮想ルータを構成する相手装置と本装置で仮想ルータの状態を確認し，マスタとなっている装置が 1 台であり，ほかの装置はバックアップになっていることを確認してください。	同一仮想ルータを構成する装置間で，マスタとなっている装置が 1 台だけであり，そのほかはバックアップとなっている場合には，次の点を確認してください。 • 仮想ルータの配下に，ほかのルータを介さずに端末が接続されている場合，各端末のネットワーク設定でデフォルトゲートウェイとして仮想ルータの仮想 IP アドレスが設定されていることを確認してください。 • 本装置を含めた通信経路上の装置での経路情報を確認してください。 端末の設定に問題がなく，通信経路上の装置での経路情報も問題ない場合は，項番 2 へ。
		仮想ルータの状態が正しくない場合は項番 3 へ。
2	show vlan コマンドで detail パラメータを指定し，仮想ルータが設定されている VLAN 内の物理ポートの状態が Forwarding であることを確認してください。	• 物理ポートの状態が Blocking の場合，STP のトポロジチェンジなどによって，一時的に通信が遮断されている可能性があります。しばらく待ってから，再度物理ポートの状態が Forwarding であることを確認してください。しばらく待っても物理ポートの状態が Forwarding にならない場合は，コンフィグレーションおよび物理的なネットワーク構成を確認してください。 • 物理ポートの状態が down の場合，物理的に接続されていません。コネクタの接続やケーブルに問題がないか，確認してください。
		物理ポートの状態が Forwarding の場合は，ルーティング先ネットワークの負荷が高くないか，確認してください。
3	同一仮想ルータを構成する相手装置と本装置の仮想ルータの状態が，お互いにマスタとなっていないことを確認してください。	複数の仮想ルータがマスタとなっている場合は項番 6 へ。
		複数の仮想ルータがマスタとなっていない場合は項番 10 へ。
4	show vrrpstatus コマンドで detail パラメータを指定し，仮想ルータが追従するプライマリ仮想ルータが設定されているか確認してください。	追従するプライマリ仮想ルータが設定されている場合は，項番 5 へ。
		追従するプライマリ仮想ルータが設定されていない場合は，項番 6 へ。
5	show vrrpstatus コマンドで detail パラメータを指定し，従っているプライマリ仮想ルータの VLAN，VRID が仮想ルータを構成している装置間で同一か確認してください。	プライマリ仮想ルータの VLAN，VRID が仮想ルータを構成する装置間で異なる場合，複数の仮想ルータがマスタになります。仮想ルータを構成する装置のコンフィグレーションは必ず合わせてください。
		プライマリ仮想ルータの VLAN，VRID が仮想ルータを構成する装置間で同一の場合は，項番 6 へ。 ただし，項番 6 以降は，プライマリ仮想ルータについて確認してください。
6	ping コマンドで，仮想ルータを構成するルータ間の通信を実 IPv4 アドレスで確認してください。	仮想ルータを構成するルータ間の実 IPv4 アドレスによる通信ができない場合，物理的なネットワーク構成を確認してください。
		ping コマンドで，仮想ルータを構成するルータ間の実 IPv4 アドレスによる通信を確認できた場合は項番 7 へ。

項番	確認内容・コマンド	対応
7	show logging コマンド，および show vrrpstatus コマンドでの statistics パラメータ指定で，ADVERTISEMENT パケットの受信状況を確認してください。	• 「Virtual router <VRID> of <Interface Name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router.」が種別ログに登録されており，統計情報の "<Number of packets> with bad advertisement interval" が増加する場合は，本装置と相手装置で ADVERTISEMENT パケット送信間隔の設定値が一致していることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check.」が種別ログに登録されており，統計情報の " <Number of packets> with authentication failed" が増加する場合は，本装置と相手装置で認証パスワードの設定内容が一致していることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet with IP TTL not equal to 255.」が種別ログに登録されており，統計情報の " <Number of packets> with bad ip ttl" が増加する場合は，本装置と相手装置間にほかのルータがないことを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet for which the address list does not match the locally configured list for the virtual router.」が種別ログに登録されており，統計情報の " <Number of packets> with bad ip address list" が増加する場合は，仮想 IP アドレスの設定が同一であることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check.」が種別ログに登録されており，統計情報の " <Number of packets> with bad authentication type" が増加する場合は，本装置と相手装置で認証パスワードの設定有無を確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that length less than the length of the VRRP header.」が種別ログに登録されており，統計情報の " <Number of packets> with packet length error" が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同一であることを確認してください。 • 「VRRP packet received with unsupported version number.」が種別ログに登録されており，統計情報の”<Number of packets> with invalid type”が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同一であることを確認してください。
		ADVERTISEMENT パケットが正常に受信されている場合は，相手装置を確認してください。 ADVERTISEMENT パケットが受信されていない場合には，項番 8 へ。
8	show interfaces コマンドで，同一仮想ルータを構成する相手装置が接続されている物理ポートの統計情報を確認してください。 また，show cpu コマンドで CPU 使用率を確認してください。	同一仮想ルータを構成する相手装置が接続されている物理ポートの Input rate および Output rate が高く，回線の負荷が高い場合，および show cpu コマンドで確認した CPU 使用率が高い場合は，以下の対策を行ってください。 • 回線がループしている場合，STP などの利用や物理的なネットワーク構成を見直してループを解消してください。 • コンフィグレーションコマンド vrrp timers advertise で ADVERTISEMENT パケットの送出間隔を長めに設定してください。 • コンフィグレーションコマンド vrrp preempt delay で自動切り戻し抑止時間を設定してください。
		物理ポートの負荷が低い場合は項番 9 へ。
9	フィルタの設定で ADVERTISEMENT パケットを廃棄する設定がないことを確認してください。	該当するフィルタの設定がある場合，ADVERTISEMENT パケットを廃棄しないようにフィルタの設定を変更してください。
		フィルタの設定がない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。

項番	確認内容・コマンド	対応
10	障害監視インタフェース設定がある場合，障害監視インタフェースの状態を確認してください。	障害監視インタフェースを設定したインタフェースに別の仮想ルータの設定があり，その仮想ルータの障害監視インタフェースが該当仮想ルータのインタフェースになっていないことを確認してください。なっている場合は，どちらかの障害インタフェースの設定を削除してください。
		上記の障害監視インタフェースの設定がない場合は項番 11 へ。
11	show vrrpstatus コマンドで detail パラメータを指定し，仮想ルータの状態が Initial でないことを確認してください。	仮想ルータの状態が Initial の場合は，次の点を確認してください。 • 現在の優先度が 0 でない場合，Admin State 欄に表示されている非動作要因を排除してください。（非動作要因については，マニュアル「運用コマンドレファレンス」を参照してください。） • show logging コマンドでログを確認し，「The VRRP virtual MAC address entry can't be registered at hardware tables.」がある場合，H/W の MAC アドレステーブル設定に失敗しています。いったん該当仮想ルータのコンフィグレーションを削除し，異なる仮想ルータ番号でコンフィグレーションを設定し直すか，仮想ルータを設定する VLAN の VLAN ID を変更することで，仮想ルータが動作する可能性があります。
		仮想ルータの状態が Initial でない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。

3.14.3 IPv6 ネットワークの VRRP 構成で通信ができない

VRRP 構成で通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-64 VRRP の障害解析方法

項番	確認内容・コマンド	対応
1	同一仮想ルータを構成する相手装置と本装置で仮想ルータの状態を確認し，マスタとなっている装置が 1 台であり，ほかの装置はバックアップになっていることを確認してください。	同一仮想ルータを構成する装置間で，マスタとなっている装置が 1 台だけであり，そのほかはバックアップとなっている場合には，次の点を確認してください。 • 仮想ルータの配下に，ほかのルータを介さずに端末が接続されている場合，各端末のネットワーク設定でデフォルトゲートウェイとして仮想ルータの仮想 IP アドレスが設定されていることを確認してください。 • 本装置を含めた通信経路上の装置での経路情報を確認してください。 端末の設定に問題がなく，通信経路上の装置での経路情報も問題ない場合は，項番 2 へ。
		仮想ルータの状態が正しくない場合は項番 3 へ。
2	show vlan コマンドで detail パラメータを指定し，仮想ルータが設定されている VLAN 内の物理ポートの状態が Forwarding であることを確認してください。	• 物理ポートの状態が Blocking の場合，STP のトポロジチェンジなどによって，一時的に通信が遮断されている可能性があります。しばらく待ってから，再度物理ポートの状態が Forwarding であることを確認してください。しばらく待っても物理ポートの状態が Forwarding にならない場合は，コンフィグレーションおよび物理的なネットワーク構成を確認してください。 • 物理ポートの状態が down の場合，物理的に接続されていません。コネクタの接続やケーブルに問題がないか，確認してください。
		物理ポートの状態が Forwarding の場合は，ルーティング先ネットワークの負荷が高くないか，確認してください。
3	同一仮想ルータを構成する相手装置と本装置の仮想ルータの状態が，お互いにマスタとなっていないことを確認してください。	複数の仮想ルータがマスタとなっている場合は項番 6 へ。

項番	確認内容・コマンド	対応
		複数の仮想ルータがマスタとなっていない場合は項番 10 へ。
4	show vrrpstatus コマンドで detail パラメータを指定し，仮想ルータが追従するプライマリ仮想ルータが設定されているか確認してください。	追従するプライマリ仮想ルータが設定されている場合は，項番 5 へ。
		追従するプライマリ仮想ルータが設定されていない場合は，項番 6 へ。
5	show vrrpstatus コマンドで detail パラメータを指定し，従っているプライマリ仮想ルータの VLAN，VRID が仮想ルータを構成している装置間で同一か確認してください。	プライマリ仮想ルータの VLAN，VRID が仮想ルータを構成する装置間で異なる場合，複数の仮想ルータがマスタになります。仮想ルータを構成する装置のコンフィグレーションは必ず合わせてください。
		プライマリ仮想ルータの VLAN，VRID が仮想ルータを構成する装置間で同一の場合は，項番 6 へ。 ただし，項番 6 以降は，プライマリ仮想ルータについて確認してください。
6	ping ipv6 コマンドで，仮想ルータを構成するルータ間の通信を実 IPv6 アドレスで確認してください。	仮想ルータを構成するルータ間の実 IPv6 アドレスによる通信ができない場合，物理的なネットワーク構成を確認してください。
		ping ipv6 コマンドで，仮想ルータを構成するルータ間の実 IPv6 アドレスによる通信を確認できた場合は項番 7 へ。

項番	確認内容・コマンド	対応
7	show vrrpstatus コマンドで statistics パラメータを指定し，ADVERTISEMENT パケットの受信状況を確認してください。	• 「Virtual router <VRID> of <Interface Name> received VRRP packet for which the advertisement interval is different than the one configured for local virtual router.」が種別ログに登録されており，統計情報の "<Number of packets> with bad advertisement interval" が増加する場合は，本装置と相手装置で ADVERTISEMENT パケット送信間隔の設定値が同一であること，および VRRP 動作モードの設定が同一であることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check.」が種別ログに登録されており，統計情報の " <Number of packets> with authentication failed" が増加する場合は，本装置と相手装置で認証パスワードの設定内容が同一であることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet with IP HopLimit not equal to 255.」が種別ログに登録されており，統計情報の " <Number of packets> with bad ipv6 hoplimit" が増加する場合は，本装置と相手装置間にほかのルータがないことを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet for which the address list does not match the locally configured list for the virtual router.」が種別ログに登録されており，統計情報の " <Number of packets> with bad ipv6 address" が増加する場合は，仮想 IP アドレス，および VRRP 動作モードの設定が同一であることを確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that does not pass the authentication check.」が種別ログに登録されており，統計情報の " <Number of packets> with bad authentication type" が増加する場合は，本装置と相手装置で認証パスワードの設定有無を確認してください。 • 「Virtual router <VRID> of <Interface Name> received VRRP packet that length less than the length of the VRRP header.」が種別ログに登録されており，統計情報の " <Number of packets> with packet length error" が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同一であることを確認してください。 • 「VRRP packet received with unsupported version number.」が種別ログに登録されており，統計情報の " <Number of packets> with invalid type" が増加する場合は，本装置と相手装置で VRRP 動作モードの設定が同一であることを確認してください。
		ADVERTISEMENT パケットが正常に受信されている場合は，相手装置を確認してください。 ADVERTISEMENT パケットが受信されていない場合には項番 8 へ。
8	show interfaces コマンドで，同一仮想ルータを構成する相手装置が接続されている物理ポートの統計情報を確認してください。 また，show cpu コマンドで CPU 使用率を確認してください。	同一仮想ルータを構成する相手装置が接続されている物理ポートの Input rate および Output rate が高く，回線の負荷が高い場合，および show cpu コマンドで確認した CPU 使用率が高い場合は，以下の対策を行ってください。 • 回線がループしている場合，STP などの利用や物理的なネットワーク構成を見直してループを解消してください。 • コンフィグレーションコマンド vrrp timers advertise で ADVERTISEMENT パケットの送出間隔を長めに設定してください。 • コンフィグレーションコマンド vrrp preempt delay で自動切り戻し抑止時間を設定してください。
		物理ポートの負荷が低い場合は項番 9 へ。
9	フィルタの設定で ADVERTISEMENT パケットを廃棄する設定がないことを確認してください。	該当するフィルタの設定がある場合，ADVERTISEMENT パケットを廃棄しないようにフィルタの設定を変更してください。
		フィルタの設定がない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。

項番	確認内容・コマンド	対応
10	障害監視インタフェース設定がある場合，障害監視インタフェースの状態を確認してください。	障害監視インタフェースを設定したインタフェースに別の仮想ルータの設定があり，その仮想ルータの障害監視インタフェースが該当仮想ルータのインタフェースになっていないことを確認してください。なっている場合は，どちらかの障害インタフェースの設定を削除してください。
		上記の障害監視インタフェースの設定がない場合は項番 11 へ。
11	show vrrpstatus コマンドで detail パラメータを指定し，仮想ルータの状態を確認してください。	仮想ルータの状態が Initial の場合は，次の点を確認してください。 • 現在の優先度が 0 でない場合，Admin State 欄に表示されている非動作要因を排除してください。（非動作要因については，マニュアル「運用コマンドレファレンス」を参照してください。） • show logging コマンドでログを確認し，「The VRRP virtual MAC address entry can't be registered at hardware tables.」がある場合，H/W の MAC アドレステーブル設定に失敗しています。いったん該当仮想ルータのコンフィグレーションを削除し，異なる仮想ルータ番号でコンフィグレーションを設定し直すか，仮想ルータを設定する VLAN の VLAN ID を変更することで，仮想ルータが動作する可能性があります。
		仮想ルータの状態が Initial でない場合，同一の仮想ルータを構成する相手装置の動作を確認してください。

3.14.4　アップリンク・リダンダント構成で通信ができない

アップリンク・リダンダント構成で通信ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-65　アップリンク・リダンダントの障害解析方法

項番	確認内容・コマンド	対応
1	show switchport-backup コマンドでプライマリポートとセカンダリポートが正しく Forwarding ／ Blocking になっていることを確認してください。	プライマリポートとセカンダリポートのどちらにも Forwarding が存在しない場合。 • Blocking の場合は，アクティブポート固定機能が動作している可能性があります。show switchport-backup コマンドで，アクティブポート固定機能が動作していないか，確認してください。アクティブポート固定機能が動作中の場合，プライマリポートがリンクアップするまで待ってください。または，set switchport-backup active コマンドで，セカンダリポートをアクティブにしてください。 • Down の場合は回線状態を確認してください。確認方法は「3.5　ネットワークインタフェースの通信障害」を参照してください。
		Forwarding/Blocking に問題がない場合，項番 2 へ。
2	アップリンク・リダンダントの上位装置を確認してください。	上位装置がフラッシュ制御フレーム受信機能をサポートしていない場合，アップリンク・リダンダントを使用している装置で MAC アドレスアップデート機能が有効になっているか，確認してください。MAC アドレスアップデート機能が有効になっていない場合，または MAC アドレスアップデートフレームが受信できないネットワーク構成の場合，アップリンク・リダンダントによる切り替えおよび切り戻しが発生すると，上位装置では MAC アドレステーブルがエージングアウトするまで，通信が回復しないことがあります。このような場合は，しばらく待ってから再度通信の状態を確認してください。または，上位装置で，MAC アドレステーブルのクリアを実施してください。
		上位装置がフラッシュ制御フレーム受信機能をサポートしている場合，項番 3 へ。

項番	確認内容・コマンド	対応
3	フラッシュ制御フレームの送信先 VLAN の設定が正しいか確認してください。	show switchport-backup コマンドで，フラッシュ制御フレームの送信先 VLAN がコンフィグレーションで設定したとおりに表示されることを確認してください。 意図したとおり表示されない場合，コンフィグレーションの設定が正しくありません。コンフィグレーションで設定したフラッシュ制御フレームの送信先 VLAN と，プライマリポートおよびセカンダリポートに設定してある VLAN を確認してください。
		フラッシュ制御フレームの送信先 VLAN の設定が正しい場合，項番 4 へ。
4	フラッシュ制御フレームが上位装置で受信できているか確認してください。	上位装置でフラッシュ制御フレームを受信しているか，show logging コマンドで確認してください。受信していない場合，フラッシュ制御フレームを受信できる VLAN が設定されているか，確認してください。

3.15 SNMP の通信障害

3.15.1 SNMP マネージャから MIB の取得ができない

コンフィグレーションが正しく設定されていることを確認してください。

SNMPv1，または SNMPv2C を使用する場合

コンフィグレーションコマンド show access-list を実行し，コンフィグレーションのアクセスリストに SNMP マネージャの IP アドレスが設定されているかどうかを確認してください。その後，コンフィグレーションコマンド show snmp-server を実行し，コミュニティ名とアクセスリストが正しく設定されているかどうかを確認してください。
設定されていない場合は，コンフィグレーションコマンド snmp-server community を実行して，SNMP マネージャに関する情報を設定してください。

```
(config)# show access-list
 access-list enable
 access-list 1 permit ip 20.1.1.1 0.0.0.255
 !
(config)# show snmp-server
 snmp-server community "event-monitor" ro 1
 !
(config)#
```

SNMPv3 を使用する場合

コンフィグレーションコマンド show snmp-server を実行し，本装置のコンフィグレーションに SNMP に関する情報が正しく設定されているかどうかを確認してください。正しく設定されていない場合は，以下のコンフィグレーションコマンドを実行して，SNMP に関する情報を設定してください。

- snmp-server engineID local
- snmp-server view
- snmp-server user
- snmp-server group

```
(config)# show snmp-server
  snmp-server engineID local "engine-ID"
  snmp-server group "v3group" v3 priv read "view1" write "view1"
  snmp-server user "v3user" "v3group" v3 auth md5 "abc*_1234" priv des "xyz/
+6789"
  snmp-server view "view1" 1.3.6.1.2.1.1 included
  !
(config)#
```

3.15.2 SNMP マネージャでトラップが受信できない

コンフィグレーションが正しく設定されていることを確認してください。

SNMPv1，または SNMPv2C を使用する場合

コンフィグレーションコマンド show snmp-server を実行し，本装置のコンフィグレーションに SNMP マネージャおよびトラップに関する情報が設定されているかどうかを確認してください。
設定されていない場合は，コンフィグレーションコマンド snmp-server host を実行して，SNMP マネージャおよびトラップに関する情報を設定してください。

```
(config)# show snmp-server
 snmp-server host    20.1.1.1 traps "event-monitor" snmp
 !
(config)#
```

SNMPv3 を使用する場合

コンフィグレーションコマンド show snmp-server を実行し，本装置のコンフィグレーションに SNMP に関する情報およびトラップに関する情報が正しく設定されているかどうかを確認してください。正しく設定されていない場合は，以下のコンフィグレーションコマンドを実行して，SNMP に関する情報およびトラップに関する情報を設定してください。

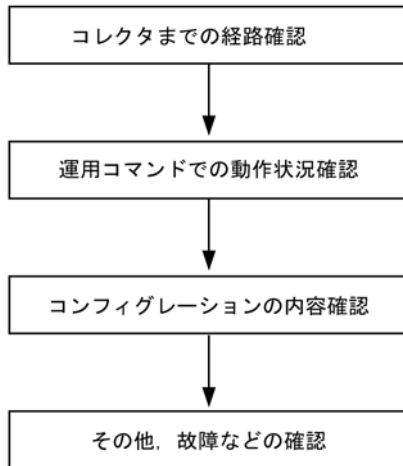
- snmp-server engineID local
- snmp-server view
- snmp-server user
- snmp-server group
- snmp-server host

```
(config)# show snmp-server
  snmp-server engineID local "engine-ID"
  snmp-server group "v3group" v3 priv notify "view1"
  snmp-server host   20.1.1.1 traps "v3user" version 3 priv snmp
  snmp-server user "v3user" "v3group" v3 auth md5 "abc*_1234" priv des "xyz/
+6789"
  snmp-server view "view1" 1.3.6.1 included
  !
(config)#
```

一部 SNMP マネージャシステムでは，SNMPv2C，SNMPv3 で発行された ospf，bgp のトラップを受信できない場合があります。その場合は，マニュアル「MIB レファレンス」に記載されている各トラップのオブジェクト ID に合わせて，SNMP マネージャのトラップ受信設定を見直してください。

3.16 sFlow 統計（フロー統計）機能のトラブルシューティング

本装置で，sFlow 統計機能のトラブルシューティングをする場合の流れは次のとおりです。

図 3-18 sFlow 統計機能のトラブルシューティングの流れ

3.16.1 sFlow パケットがコレクタに届かない

(1) コレクタまでの経路確認

「3.7.1 通信できない，または切断されている」および「3.10.1 通信できない，または切断されている」を参照し，コレクタに対してネットワークが正しく接続されているかを確認してください。もし，コンフィグレーションで sFlow パケットの最大サイズ（max-packet-size）を変更している場合は，指定しているパケットサイズでコレクタまで接続できるか確認してください。

(2) 運用コマンドでの動作確認

show sflow コマンドを数回実行して sFlow 統計情報を表示し，sFlow 統計機能が稼働しているか確認してください。下線部の値が増加していない場合は，「(3) コンフィグレーションの確認」を参照してください。増加している場合は，「3.7.1 通信できない，または切断されている」，「3.10.1 通信できない，または切断されている」および「(5) コレクタ側の設定確認」を参照し，コレクタに対してネットワークが正しく接続されているかを確認してください。

図 3-19 show sflow コマンドの表示例

```
> show sflow
Date 20XX/12/24 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  16:00:05
sFlow agent data :
  sFlow service version  : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate    : 1 per 2048 packets
  Configured sFlow ingress ports :  1/2-4
  Configured sFlow egress ports  :  2/9-11
  Received sFlow samples : 37269  Dropped sFlow samples(Dropped Que) :
```

```
2093(2041)
  Exported sFlow samples : 37269  Couldn't exported sFlow samples    :       0
sFlow collector data :
  Collector IP address: 192.168.4.199  UDP:6343  Source IP address: 130.130.130.1
  Send FlowSample UDP packets    : 12077  Send failed packets:     0
  Send CounterSample UDP packets:    621  Send failed packets:     0
  Collector IP address: 192.168.4.203  UDP:65535  Source IP address: 130.130.130.1
  Send FlowSample UDP packets    : 12077  Send failed packets:     0
  Send CounterSample UDP packets:    621  Send failed packets:     0
>
```

注　下線部の値が，増加していることを確認してください。

(3) コンフィグレーションの確認

以下の内容について，運用中のコンフィグレーションを確認してください。

- コンフィグレーションに，sFlow パケットの送信先であるコレクタの IP アドレスと UDP ポート番号が正しく設定されていることを確認してください。

図 3-20　コンフィグレーションの表示例 1

```
(config)# show sflow
sflow destination 192.1.1.1 6455    ←コレクタの情報が正しく設定されていること
sflow sample 2048
!
(config)#
```

- サンプリング間隔が設定されていることを確認してください。
  サンプリング間隔が設定されていないと，デフォルト値（＝大きな値）で動作するため値が大き過ぎ，フローサンプルがコレクタにほとんど送信されません。そのため，適切なサンプリング間隔を設定してください。ただし，推奨値より極端に小さな値を設定した場合，CPU 使用率が高くなる可能性があります。

図 3-21　コンフィグレーションの表示例 2

```
(config)# show sflow
sflow destination 192.1.1.1 6455
sflow sample 2048      ←適切なサンプリング間隔が設定されていること
!
(config)#
```

図 3-22　運用コマンドの表示例

```
> show sflow
Date 20XX/12/24 20:04:01 UTC
sFlow service status: enable
Progress time from sFlow statistics cleared:  16:00:05
  sFlow agent data :
  sFlow service version  : 4
  CounterSample interval rate: 60 seconds
  Default configured rate: 1 per 2048 packets
  Default actual rate    : 1 per 2048 packets
  Configured sFlow ingress ports :  1/2-4
  Configured sFlow egress ports  :  2/9-11
  Received sFlow samples : 37269  Dropped sFlow samples(Dropped Que) :
2093(2041)
  Exported sFlow samples : 37269  Couldn't exported sFlow samples    :       0
                           :
>
```

注　下線部に，適切なサンプリング間隔が表示されていることを確認してください。

● フロー統計を行いたい物理ポートに対し，"sflow forward" が設定されていることを確認してください。

図 3-23　**コンフィグレーションの表示例** 3

```
(config)# show interfaces
interface gigabitethernet 1/2
  switchport mode access
  sflow forward ingress      ←ここに"sflow forward"が設定されていること
!
(config)#
```

● フロー統計を行いたい物理ポートに対し，"filter" が設定されていないことを「3.22.1　フィルタ /QoS 設定情報の確認」を参照して確認してください。

● "sflow source" によって，sFlow パケットの送信元（エージェント）IP アドレスを指定した場合，その IP アドレスが本装置のポートに割り付けられていることを確認してください。

図 3-24　**コンフィグレーションの表示例** 4

```
(config)# show sflow
sflow destination 192.1.1.1 6455
sflow sample 2048
sflow source 192.1.1.100     ←本装置のポートに割り付けられているIPアドレスであること
!
(config)#
```

(4) NIF 状態・ポート状態の確認

show interfaces コマンドを実行し，sFlow 統計で監視する本装置の物理ポートやコレクタとつながる物理ポートの up/down 状態が，"active"（正常動作中）であることを確認してください。

図 3-25　**ポート状態の表示例**

```
> show interfaces gigabitethernet 1/5
Date 20XX/12/24 17:19:34 UTC
NIF1: active  24-port 10BASE-T/100BASE-TX/1000BASE-T    retry:0
Port5: active up  100BASE-TX full(auto)    0012.e220.ec31
  Time-since-last-status-change:1:47:47
    Bandwidth:10000kbps  Average out:5Mbps  Average in:5Mbps
    Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
    Output rate:    4893.5kbps       16.8kpps
    Input  rate:    4893.5kbps       16.8kpps
    Flow control send   :off
    Flow control receive:off
    TPID:8100
                              :
>
```

注　下線部が，"active"または"active up"であることを確認してください。

ポートが DOWN 状態の場合は，「3.7.1　通信できない，または切断されている」および「3.10.1　通信できない，または切断されている」を参照してください。

(5) コレクタ側の設定確認

- コレクタ側で UDP ポート番号（デフォルト値は 6343）が受信可能になっているか確認してください。受信可能になっていない場合，ICMP（[Type]Destination Unreachable [Code]Port Unreachable）が本装置に送られます。
- その他，利用しているコレクタ側の設定が正しいか確認してください。

3.16.2 フローサンプルがコレクタに届かない

「3.16.1 sFlow パケットがコレクタに届かない」を確認しても解決しない場合は，以下を確認してください。

(1) 中継パケット有無の確認

show interfaces コマンドを実行し，パケットが中継されているか確認してください。

図 3-26 ポート状態の表示例

```
> show interfaces gigabitethernet 1/5
Date 20XX/12/24 17:19:34 UTC
NIF1: active  24-port 10BASE-T/100BASE-TX/1000BASE-T    retry:0
Port5: active up  100BASE-TX full(auto)    0012.e220.ec31
  Time-since-last-status-change:1:47:47
    Bandwidth:10000kbps  Average out:5Mbps  Average in:5Mbps
    Peak out:5Mbps at 15:44:36  Peak in:5Mbps at 15:44:18
    Output rate:    4893.5kbps       16.8kpps
    Input  rate:    4893.5kbps       16.8kpps
    Flow control send   :off
    Flow control receive:off
    TPID:8100
                                                :
>
```

注 下線部の表示で，パケットが中継されていることを確認してください。

(2) コレクタ側の設定確認

利用しているコレクタ側の設定が正しいか確認してください。

3.16.3 カウンタサンプルがコレクタに届かない

「3.16.1 sFlow パケットがコレクタに届かない」を確認しても解決しない場合は，以下を確認してください。

(1) カウンタサンプルの送信間隔の確認

本装置のコンフィグレーションで，フロー統計に関するカウンタサンプルの送信間隔の情報が 0 になっていないかを確認してください。この値が 0 になっているとカウンタサンプルのデータがコレクタへ送信されません。

図 3-27 コンフィグレーションの表示例

```
(config)# show sflow
sflow destination 192.1.1.1 6455
sflow sample 2048
sflow polling-interval 60      ←ここに0が設定されていないこと
!
(config)#
```

3.17　隣接装置管理機能の通信障害

3.17.1　LLDP 機能により隣接装置情報が取得できない

LLDP 機能で隣接装置の情報が正しく取得できない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-66　LLDP 機能使用時の障害解析方法

項番	確認内容・コマンド	対応
1	show lldp コマンドを実行し，LLDP 機能の動作状態を確認してください。	Status が Enabled の場合は項番 2 へ。
		Status が Disabled の場合は LLDP 機能が停止状態となっています。LLDP 機能を有効にしてください。
2	show lldp コマンドを実行し，ポート情報を確認してください。	隣接装置が接続されているポート情報が表示されている場合は項番 3 へ。
		隣接装置が接続されているポート情報が表示されていない場合は，該当ポートが LLDP 機能の動作対象外となっています。該当ポートに対し LLDP 機能を有効にしてください。
3	show lldp statistics コマンドを実行し，隣接装置が接続されているポートの統計情報を確認してください。	Tx カウントは増加し Rx カウントが増加しない場合は，隣接装置側でも項番 1 から項番 3 を調査してください。隣接装置側でも Tx カウントが増加している場合は，装置間の接続が誤っている可能性があるので接続を確認してください。
		Discard カウントが増加している場合は，装置間の接続を確認してください。
		その他の場合は項番 4 へ。
4	show lldp コマンドを実行し，隣接装置が接続されているポート情報のポート状態を確認してください。	Link が Up 状態の場合は項番 5 へ。
		Link が Down 状態の場合は回線状態を確認してください。確認方法は「3.5　ネットワークインタフェースの通信障害」を参照してください。
5	show lldp コマンドを実行し，隣接装置が接続されているポートの隣接装置情報数を確認してください。	Neighbor Counts が 0 の場合は隣接装置側で項番 1 から項番 5 を調査してください。隣接装置側でも隣接装置情報数が 0 の場合は，装置間の接続が誤っている可能性があるので接続を確認してください。 また，フィルタまたは QoS 制御によって LLDP の制御フレームが廃棄されている可能性があります。「3.22.1　フィルタ /QoS 設定情報の確認」を参照し確認してください。

3.17.2　OADP 機能により隣接装置情報が取得できない

OADP 機能で隣接装置の情報が正しく取得できない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-67　OADP 機能使用時の障害解析方法

項番	確認内容・コマンド	対応
1	show oadp コマンドを実行し，OADP 機能の動作状態を確認してください。	Status が Enabled の場合は項番 2 へ。

項番	確認内容・コマンド	対応
		Status が Disabled の場合は OADP 機能が停止状態となっています。OADP 機能を有効にしてください。
2	show oadp コマンドを実行し，ポート情報の表示を確認してください。	Enabled Port に隣接装置が接続されているポート情報が表示されている場合は項番 3 へ。
		Enabled Port に隣接装置が接続されているポートが表示されていない場合は OADP 機能の動作対象外となっています。ポートに対し OADP 機能を有効にしてください。なお，チャネルグループに属するポートでは OADP 機能の対象外となります。チャネルグループに対して OADP 機能を有効にしてください。
3	show oadp statistics コマンドを実行し，隣接装置が接続されているポートの統計情報を確認してください。	Tx カウントは増加し Rx カウントが増加しない場合は隣接装置側でも項番 1 から項番 3 を調査してください。隣接装置側でも Tx カウントが増加している場合は，装置間の接続が誤っている可能性がありますので接続を確認してください。
		Discard/ERR カウントが増加している場合は，装置間の接続を確認してください。
		その他の場合は項番 4 へ。
4	show interfaces コマンドを実行し，隣接装置が接続されているポートの状態を確認してください。	該当するポートの状態が active up の場合は項番 5 へ。
		その他の場合は「3.5　ネットワークインタフェースの通信障害」を参照してください。
5	show vlan コマンドを実行し，隣接装置が接続されているポートの所属する VLAN の状態を確認してください。	Status が Up の場合は項番 6 へ。
		Status が Disable の場合は OADP 機能の動作対象外になります。VLAN の状態を有効にしてください。
		その他の場合は「3.6　レイヤ 2 ネットワークの通信障害」を参照してください。
6	show oadp コマンドを実行し，隣接装置が接続されているポートの隣接装置情報を確認してください。	表示されない場合は隣接装置側で項番 1 から項番 6 を調査してください。隣接装置側でも該当ポートの隣接装置情報が表示されない場合は，装置間の接続が誤っている可能性があるため，接続を確認してください。また，フィルタまたは QoS 制御によって OADP の制御フレームが廃棄されている可能性があります。「3.22.1　フィルタ /QoS 設定情報の確認」を参照し確認してください。

3.18　NTP の通信障害

3.18.1　NTP による時刻同期ができない

NTP による時刻同期ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-68　NTP の障害解析方法

項番	確認内容・コマンド	対応
1	show clock コマンドでタイムゾーンの設定があることを確認してください。	コマンドの表示結果にタイムゾーンが設定されている場合は項番 2 へ。
		コマンドの表示結果にタイムゾーンが設定されていない場合はタイムゾーンの設定をしてください。
2	本装置と NTP サーバとの時刻差を確認してください。	本装置と NTP サーバとの時刻差が 1000 秒以内の場合は項番 3 へ。
		本装置と NTP サーバとの時刻差が 1000 秒以上ある場合には，set clock コマンドを使用して本装置の時刻を NTP サーバと合わせてください。
3	NTP サーバとの IPv4 による通信を確認してください。	NTP サーバと本装置間で IPv4 の通信が可能か，ping コマンドで確認してください。
		NTP サーバまたは本装置の設定で，UDP ポート番号 123 のパケットを廃棄する設定がないことを確認してください。

3.19 IEEE802.3ah/UDLD 機能の通信障害

3.19.1 IEEE802.3ah/UDLD 機能でポートが inactive 状態となる

IEEE802.3ah/UDLD 機能によってポートが inactive 状態となる場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-69 IEEE802.3ah/UDLD 機能使用時の障害解析方法

項番	確認内容・コマンド	対応
1	show efmoam コマンドを実行し，IEEE802.3ah/UDLD 機能で inactive 状態にしたポートの障害種別を確認してください。	Link status に "Down(loop)" が表示されている場合は，L2 ループが起こる構成となっている可能性があります。ネットワーク構成を見直してください。
		Link status に "Down(uni-link)" が表示されている場合は，項番 2 へ。
2	対向装置で IEEE802.3ah/OAM 機能が有効であることを確認してください。	対向装置側で IEEE802.3ah/OAM 機能が有効となっていない場合は，有効にしてください。
		対向装置側で IEEE802.3ah/OAM 機能が有効となっている場合は項番 3 へ。
3	show efmoam statistics コマンドを実行し，禁止構成となっていないことを確認してください。	Info TLV の Unstable がカウントアップされている場合は，IEEE802.3ah/UDLD 機能での禁止構成となっている可能性があります。該当物理ポートの接続先の装置が 1 台であることを確認してください。
		Info TLV の Unstable がカウントアップされていない場合は項番 4 へ。
4	対向装置と直接接続されていることを確認してください。	メディアコンバータやハブなどが介在している場合は，対向装置と直接接続できるようネットワーク構成を見直してください。どうしても中継装置が必要な場合は，両側のリンク状態が連動するメディアコンバータを使用してください（ただし，推奨はしません）。
		直接接続されている場合は項番 5 へ。
5	show efmoam コマンドを実行し，障害を検出するための応答タイムアウト回数を確認してください。	udld-detection-count が初期値未満の場合，実際に障害となっていない場合でも片方向リンク障害を誤検出する可能性が高まります。この値を変更してください。
		udld-detection-count が初期値以上の場合は項番 6 へ。
6	フィルタ，QoS 制御の設定を確認してください。	フィルタまたは QoS 制御によって IEEE802.3ah/UDLD 機能で使用する制御フレーム（slow-protocol）が廃棄されている可能性があります。「3.22.1 フィルタ /QoS 設定情報の確認」を参照し確認してください。問題がない場合は項番 7 へ。
7	回線のテストをしてください。	「5.1 回線をテストする」を参照し，回線のテストをしてください。問題がない場合は項番 8 へ。
8	ケーブルを確認してください。	ケーブル不良の可能性があります。該当ポートで使用しているケーブルを交換してください。

注 IEEE802.3ah/OAM：IEEE802.3ah で規定されている OAM プロトコル
IEEE802.3ah/UDLD：IEEE802.3ah/OAM を使用した，本装置特有の片方向リンク障害検出機能

3.20 省電力機能のトラブル

3.20.1 スケジュールが動作しない

スケジュールが動作しない場合は，以下に従って確認してください。

1. show power-control schedule コマンドを実行して，表示されるスケジュールに現在時刻が含まれているか確認し，次の表に従って原因の切り分けを行ってください。

表 3-70 スケジューリングを使用した省電力機能のトラブルおよび対応

項番	表示結果	確認内容	原因	対応
1	現在時刻が含まれない	コンフィグレーションコマンド schedule-power-control time-range の設定を確認してください。	コンフィグレーションコマンド schedule-power-control time-range が正しく設定されていません。	• 現在時刻を含むエントリが指定されていない場合，現在時刻を含むエントリを指定してください。 • 現在時刻を含むエントリの action が disable 指定されている場合，disable 指定されているエントリを削除してください。
2	現在時刻が含まれる	コンフィグレーション schedule-power-control で設定した機能と通常時間帯に設定した機能が一致していないか確認してください。一致している場合，原因と対応欄を参照してください。	すでにコンフィグレーション schedule-power-control で設定した機能で動作しています。	コンフィグレーション schedule-power-control の設定を確認してください。
3		show logging コマンドでログを参照して，スケジュールの開始・終了時刻の 30 分前以降にシステム時刻を変更していないか確認してください。システム時刻を変更していた場合，原因と対応欄を参照してください。	システム時刻の変更によって，スケジュール誤差が発生しています。	30 分以内にスケジュールが自動的に開始されますので，そのままお待ちください。時刻変更に関する注意は，マニュアル「コンフィグレーションガイド」を参照してください。

3.21　CPU で処理するパケットの輻輳が回復しない

CPU で処理するパケットの輻輳が回復しない場合の対処方法について説明します。

CPU で処理するパケットの輻輳は，ソフトウェア処理が必要なパケットを多数受信した場合に，CPU 宛ての受信キューが溢れることで発生します。

CPU 宛てのキューでパケットの輻輳を検出すると，次のメッセージが出力されます。

”E3 SOFTWARE 00003301 1000:000000000000 CPU congestion detected.”

パケットの輻輳が回復すると，次のメッセージが出力されます。

”E3 SOFTWARE 00003302 1000:000000000000 CPU has recovered from congestion.”

CPU で処理するパケットの輻輳は，経路情報のエージングによって一時的に宛先不明のパケットを大量に受信した場合など，正常に動作していても発生することがあります。パケットの輻輳が回復しない，またはパケットの輻輳の発生と回復を頻繁に繰り返す場合は，本装置の設定またはネットワーク構成に問題がある可能性があります。本事象発生中に，次の表に従って対応してください。

表 3-71　CPU で処理するパケットの輻輳が回復しない場合の対処方法

項番	確認内容・コマンド	対応
1	パケット種別の特定 • show netstat statistics コマンドを 20 秒間隔で続けて実行して，結果を比較してください。	比較した結果，パケット種別が ip または ip6 の統計項目にある total packets received で大幅にカウントが増加している場合は項番 2 へ。
		比較した結果，パケット種別が arp の統計項目にある packets received で大幅にカウントが増加している場合は項番 2 へ。
		上記以外の場合は項番 4 へ。
2	受信 VLAN インタフェースの特定 • show netstat interface コマンドを 20 秒間隔で続けて実行して，結果を比較してください。	比較した結果，特定の VLAN インタフェースの統計項目にある Ipkts で大幅にカウントが増加している場合は項番 3 へ。
		上記以外の場合は項番 4 へ。
3	パケットの送信元／宛先アドレスの特定 • 項番 2 で特定した VLAN インタフェースに対して show tcpdump interface コマンドを実行して，項番 1 で特定したパケット種別の送信元アドレスと宛先アドレスを確認してください。	パケット種別が ip または ip6 で該当パケットの宛先アドレスが本装置の場合は，不正に送信されている可能性があります。送信元アドレスを持つ端末の設定を見直すか，ネットワーク構成を見直して，本装置宛てに該当パケットが送信されないようにしてください。
		パケット種別が ip または ip6 で該当パケットの宛先アドレスが他装置の場合は，ARP 情報のアドレスが解決していない，または宛先不明のパケットを大量に受信していることが考えられます。 • パケット種別が ip の場合は，「3.7.1　通信できない，または切断されている　(5) 隣接装置との ARP 解決情報の確認」を参照してください。 • パケット種別が ip6 の場合は，「3.10.1　通信できない，または切断されている　(5) 隣接装置との NDP 解決情報の確認」を参照してください。
		パケット種別が arp の場合は，ARP パケットを大量に受信しています。この場合，L2 ループ構成となっている可能性があります。ネットワーク構成を見直してください。ネットワーク構成に問題がなければ，送信元アドレスを持つ端末の設定を見直してください。

項番	確認内容・コマンド	対応
4	解析情報の採取 • show tech-support コマンドを 2 回実行してください。	収集した情報を支援部署に送付してください。

3.22　フィルタ /QoS の設定により生じる通信障害

3.22.1　フィルタ /QoS 設定情報の確認

本装置を使用しているネットワーク上で通信トラブルが発生する要因として，フィルタによって特定のパケットが廃棄されているか，または QoS 制御の帯域監視，廃棄制御もしくはシェーパによってパケットが廃棄されている可能性が考えられます。

フィルタおよび QoS 制御によって本装置内でパケットが廃棄されている場合に，廃棄個所を特定する方法の手順を次に示します。

また，フィルタの動作に指定しているポリシーベースルーティングがデフォルト動作に従っていて，かつデフォルト動作が廃棄の場合は，フィルタによるパケット廃棄と同じ扱いとなります。次の手順に加えて，「3.24.1　ポリシーベースルーティングで中継されない場合の確認方法」を参照してください。

（1）フィルタによるパケット廃棄の確認方法

1. 本装置にログインします。
2. show access-filter コマンドを実行し，インタフェースに適用しているアクセスリストのフィルタ条件とフィルタ条件に一致したパケット数，暗黙の廃棄のフィルタエントリで廃棄したパケット数を確認します。
3. 2. で確認したフィルタ条件と通信できないパケットの内容を比較して，該当パケットを廃棄していないか，またはポリシーベースルーティングを実行していないか確認します。通信できないパケットの内容が，適用しているすべてのフィルタ条件に一致していない場合，暗黙的に廃棄している可能性があります。
4. フィルタのコンフィグレーションの設定条件が正しいかを見直してください。
5. コンフィグレーションが正しく設定されている場合は，アクセスリストロギングを使って，廃棄したパケットの情報を確認してください。

（2）QoS 制御の帯域監視によるパケット廃棄の確認方法

1. 本装置にログインします。
2. show qos-flow コマンドを実行し，インタフェースに適用している帯域監視のフロー検出条件と動作指定，フロー検出条件に一致したパケット数を確認します。
3. 2. で確認したフロー検出条件と通信できないパケットの内容を比較して，該当パケットを廃棄していないか確認します。最大帯域制御を違反したパケットは廃棄し，統計情報の "matched packets(max-rate over)" をカウントアップします。本統計情報をカウントアップしている場合，インタフェースに適用している帯域監視によって，パケットを廃棄している可能性があります。
4. QoS 制御のコンフィグレーションの設定条件が正しいか，およびシステム構築での帯域監視の設定が適切であるかを見直してください。

（3）QoS 制御の廃棄制御およびレガシーシェーパによるパケット廃棄の確認方法

1. 本装置にログインします。
2. show qos queueing コマンドを使って，出力インタフェースの統計情報の "discard packets" を確認してください。
3. 2. で確認した統計情報がカウントアップしている場合，QoS 制御の廃棄制御およびレガシーシェーパによってパケットを廃棄しています。
4. 廃棄制御およびレガシーシェーパのシステム運用が適切であるかを見直してください。

3.23 DHCP snooping のトラブル

3.23.1 DHCP に関するトラブル

DHCP snooping 構成で DHCP の IP アドレス配布ができない場合は，次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-72 DHCP snooping 構成で DHCP の IP アドレス配布ができない場合の障害解析方法

項番	確認内容	対応
1	show logging コマンドを実行して，運用ログにハードウェア障害が記録されていないかを確認してください。	運用ログにハードウェア障害が記録されていた場合は，装置を交換してください。
		上記に該当しない場合は項番 2 へ。
2	IP アドレスの新規配布ができないのか，IP アドレス更新だけができないのか確認してください。	IP アドレスが配布できない場合は，項番 3 へ。
		IP アドレスが更新できない場合は，項番 9 へ。
3	show ip dhcp snooping statistics コマンドを実行し，DHCP snooping の動作状況を確認してください。	DHCP snooping が有効な untrust ポートとして表示されるポートが，対象装置（IP アドレスが配布できない装置）に接続されているポートと一致している場合は，項番 4 へ。
		それ以外のポートに接続されている場合は，DHCP snooping の対象外となっています。 ネットワーク構成や DHCP サーバなどの設定を確認して，問題が見つからない場合は項番 10 へ。
4	クライアントとサーバ間がどの形態で接続されているかを確認してください。	本装置がレイヤ 2 スイッチとしてクライアントとサーバの間に接続されている場合は，項番 8 へ。
		本装置の DHCP サーバを使用している場合は，項番 5 へ。
		本装置の DHCP リレーを使用している場合は，項番 5 へ。
		本装置とクライアントの間に DHCP リレーが存在する場合は，項番 6 へ。
		本装置とクライアントの間に Option82 を付与する装置がある場合は，項番 7 へ。
		上記の複数の条件に一致する場合は，該当する項番を順番に参照してください。
5	DHCP サーバ・リレーの動作が問題ないことを確認してください。	「3.7.2 DHCP 機能で IP アドレスが割り振られない」を参照して，DHCP サーバや DHCP リレーで IP アドレスが配布できる状態となっていることを確認してください。 問題がない場合は項番 8 へ。
6	DHCP リレー経由のパケットを中継する場合は，コンフィグレーションコマンド no ip dhcp snooping verify mac-address が設定されているか確認してください。	DHCP リレー経由の DHCP パケットはクライアントハードウェアアドレスと送信元 MAC アドレスが異なるため，パケットが廃棄されます。 該当パケットを中継する場合はコンフィグレーションコマンド no ip dhcp snooping verify mac-address を設定してください。
7	リレーエージェント情報オプションを含むパケットを中継する場合は，コンフィグレーションコマンド ip dhcp snooping information option allow-untrusted が設定されているか確認してください。	リレーエージェント情報オプション（Option82）を含むパケットはデフォルトでは廃棄されます。 該当パケットを中継する場合はコンフィグレーションコマンド ip dhcp snooping information option allow-untrusted を設定してください。

項番	確認内容	対応
8	DHCP サーバを接続しているポートが trust ポートになっていることを確認してください。	untrust ポートからの DHCP サーバ応答パケットは廃棄されます。 対象とする DHCP サーバが正規のものである場合，接続されているポートにコンフィグレーションコマンド ip dhcp snooping trust を設定してください。 なお，本装置の DHCP サーバを使用する場合は untrust ポートで問題ありません。また，本装置の DHCP リレーを使用する場合は，DHCP サーバが接続されている VLAN が DHCP snooping の対象外か，trust ポートになっている必要があります。
9	show ip dhcp snooping binding コマンドでバインディング情報を確認してください。	装置を再起動したあとに IP アドレス更新ができない場合は，バインディングデータベースの保存を確認してください。 「3.23.2　バインディングデータベースの保存に関するトラブル」を参照してください。
		バインディング情報で表示される該当（MAC アドレス／IP アドレスが一致する）エントリのポートや VLAN ID が異なる場合は，IP アドレスを取得したあとで接続ポートや VLAN の収容を変更した可能性があります。 現在のポートや VLAN で使用を続ける場合は，再度 IP アドレスを取得してください。
10	その他	上記のどれでも解決しない場合は，本書を参考に，装置で使用しているその他の機能を確認してください。

3.23.2 バインディングデータベースの保存に関するトラブル

装置再起動時などにバインディング情報が引き継げない場合は，バインディングデータベースの保存に関するトラブルが考えられます。次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-73　バインディングデータベースの保存に関するトラブルの障害解析方法

項番	確認内容	対応
1	show mc コマンドまたは show flash コマンドで，flash または MC に十分な未使用容量があることを確認してください。	未使用容量がない場合は，不要なファイルを消すなどして未使用容量を確保してください。
		問題が見つからない場合，項番 2 へ。
2	バインディングデータベースの保存先を確認してください。	flash に保存する場合は，項番 4 へ。
		MC に保存する場合は，項番 3 へ。
3	ls mc-dir コマンドで，MC の保存ディレクトリが存在することを確認してください。	ディレクトリが存在しない場合は，mkdir コマンドでディレクトリを作成してください。
		問題が見つからない場合，項番 4 へ。
4	コンフィグレーションコマンド ip dhcp snooping database write-delay の設定と，show ip dhcp snooping binding コマンドでバインディングデータベースの最終保存時間を確認してください。	バインディング情報が更新されても指定した時間が経過するまでバインディングデータベースは保存されません。IP アドレス配布後に指定時間が経過するのを待って，バインディングデータベースの最終保存時間が更新されていることを確認してください。
		問題が見つからない場合，項番 5 へ。

項番	確認内容	対応
5	DHCP クライアントに配布された IP アドレスのリース時間が，データベース保存時の待ち時間より長いことを確認してください。	リース時間の方が短い場合，バインディングデータベースを読み込む前に IP アドレスがリース切れとなる可能性があります。 コンフィグレーションコマンド ip dhcp snooping database write-delay で本装置のデータベース保存時の待ち時間を短くするか，DHCP サーバで IP アドレスのリース時間を長くしてください。
		問題が見つからない場合，項番 6 へ。
6	その他	バインディングデータベースを flash に保存したときは問題がなく，MC に保存したときにバインディング情報が引き継げない場合は，MC を交換してください。 なお，長期間の運用を前提とする場合は，バインディングデータベースの保存先を MC にしてください。

3.23.3　ARP に関するトラブル

ARP パケットが廃棄されていると IPv4 通信ができなくなります。ARP パケットが廃棄される原因として，ダイナミック ARP 検査が考えられます。次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-74　ダイナミック ARP 検査によって発生したトラブルの障害解析方法

項番	確認内容	対応
1	DHCP snooping 設定情報を確認してください。	「3.23.1　DHCP に関するトラブル」を参照して，DHCP snooping が正常に動作していることを確認してください。
		問題が見つからない場合，項番 2 へ。
2	show ip arp inspection statistics コマンドを実行して，ダイナミック ARP 検査の動作状況を確認してください。	ダイナミック ARP 検査が有効な untrust ポートとして表示されるポートが，IPv4 通信のできないポートと一致している場合は，項番 3 へ。
		それ以外のポートに接続されている場合は，ダイナミック ARP 検査の対象外となっています。ネットワーク構成や IPv4 通信ができない装置の設定を確認して問題が見つからない場合，項番 4 へ。
3	show ip dhcp snooping binding コマンドを実行して，通信できない装置に対するバインディング情報があるか確認してください。	バインディング情報がない場合，対象装置が固定 IP アドレスを持つ装置であれば，コンフィグレーションコマンド ip source binding を設定してください。また，DHCP によって IP アドレスを取得する装置であれば，IP アドレスを再取得してください。
4	その他	上記のどれでも解決しない場合は，本書を参考に，装置で使用しているその他の機能を確認してください。

3.23.4　DHCP，ARP 以外の通信に関するトラブル

端末フィルタを有効にした場合，バインディング情報にない装置からの DHCP/ARP 以外のすべてのパケットを廃棄します。次の表に示す障害解析方法に従って原因の切り分けを行ってください。

表 3-75　端末フィルタによって発生したトラブルの障害解析方法

項番	確認内容	対応
1	DHCP snooping 設定情報を確認してください。	「3.23.1　DHCP に関するトラブル」を参照して，DHCP snooping が正常に動作していることを確認してください。

項番	確認内容	対応
		問題が見つからない場合，項番 2 へ。
2	コンフィグレーションコマンド ip verify source が対象ポートに設定されているか確認してください。	ip verify source が設定されている場合はバインディング情報にない装置からのパケットを廃棄します。問題がない場合，項番 3 へ。
		ip verify source が設定されていない場合は，項番 4 へ。
3	show ip dhcp snooping binding コマンドを実行して，通信できない装置に対するバインディング情報があるか確認してください。	バインディング情報がない場合，対象装置が固定 IP アドレスを持つ装置であれば，コンフィグレーションコマンド ip source binding を設定してください。また，DHCP によって IP アドレスを取得する装置であれば，IP アドレスを再取得してください。
4	その他	上記のどれでも解決しない場合は，本書を参考に，装置で使用しているその他の機能を確認してください。

3.24 ポリシーベースルーティングのトラブル

3.24.1 ポリシーベースルーティングで中継されない場合の確認方法

ポリシーベースルーティンググループの使用中に，指定した経路に中継されない場合，次の表に従って対処してください。

表 3-76 ポリシーベースルーティングで中継されない場合の対処方法

項番	確認内容・コマンド	対応
1	ポリシーベースルーティングリスト情報を設定しているフィルタの動作状況を確認 • show access-filter コマンドを実行し，"matched packets :" でフィルタ条件に一致したパケット数を確認してください。	通信できないパケット数と matched packets の値が異なる場合は，フィルタの検出条件が誤っていて，暗黙の廃棄をしている可能性があります。 フィルタの設定を見直してください。
		通信できないパケット数と matched packets の値が同じ場合，項番 2 へ。
2	ポリシーベースルーティンググループの動作状況を確認 • show ip cache policy コマンドを実行し，"*>" の表示状況を確認してください。	未表示の場合，起動中またはデフォルト動作によって通常中継または廃棄している可能性があります。 起動中の確認は，項番 3 へ。
		表示されている場合，項番 4 へ。
3	ポリシーベースルーティングの経路切り替え動作状況を確認 • show ip cache policy コマンドの "Policy Base Routing Default Init Interval" の "Start Time" および "End Time" 項目の値を確認してください。	"End Time" にだけ "-" が表示されている場合，起動中のためパケットを廃棄した可能性があります。起動が完了するまでお待ちください。
		"Start Time" および "End Time" が共に "-" または日付が表示されている場合，項番 5 へ。
4	ポリシーベースルーティングの中継先の VLAN インタフェースおよびトラッキング機能の状況を確認 • show vlan コマンドを実行し，"Status:" 項目を確認してください。 • show track-object コマンドを実行し，"State" 項目のトラック状態を確認してください。	ポリシーベースルーティングの中継先の VLAN インタフェースまたはトラッキング機能の状況のどちらかが "Up" でない場合，デフォルト動作によって通常中継または廃棄しています。中継先の VLAN インタフェースおよびトラッキング機能の状況がすべて "Up" になるようにしてください。
		すべて "Up" の場合，項番 5 へ。
5	ポリシーベースルーティングの経路切り戻し動作の設定を確認 • show ip cache policy コマンドを実行し，"Recover" 項目を確認してください。	"Off" の場合，経路切り戻し動作が行われないため経路の再選択が行われない状態です。reset policy-list コマンドを実行して経路の再選択を実施してください。
		"On" の場合，項番 6 へ。
6	ポリシーベースルーティングの中継先の ARP 情報の確認 • show ip arp コマンドを実行し，中継先のネクストホップが登録されているか確認してください。 • show mac-address-table コマンドを実行し，中継先の MAC アドレスが登録されているか確認してください。	ARP が未登録の場合，スタティック ARP を設定してください。MAC アドレスが未登録の場合，MAC アドレスのスタティックエントリを設定してください。または，ポリシーベースルーティングのトラッキング機能を使用してください。
		登録済みの場合，項番 7 へ。

項番	確認内容・コマンド	対応
7	送信先インタフェースでネットワークの通信障害が発生していないか確認 • 「3.7　IPv4 ネットワークの通信障害」を参照してください。	通信障害が発生している場合，参照先の対応に従ってください。
		通信障害が発生していない場合，項番 8 へ。
8	解析情報の採取 • show tech-support コマンドおよび dump policy コマンドを順に 2 回実行してください。※	収集した情報を支援部署に送付してください。

注※
2 回目の dump policy コマンドを実行すると，1 回目に収集したメモリダンプファイルが削除されるため，1 回目に収集したメモリダンプファイルを退避してから実行してください。

3.24.2 ポリシーベースルーティングのトラッキング機能でトラック状態が想定と異なる場合の確認方法

本装置のトラック状態が想定される状態とは異なる原因として，次の三つが考えられます。

1. トラックのコンフィグレーションが変更された
2. ネットワーク障害によって，ポーリング監視トラックのトラック対象と通信できない
3. ネットワークのトラフィック負荷によって，ポーリング監視トラックのトラック対象との通信が不安定である

現在のトラック状態が想定と異なる状態になった原因を調査するには，次の表に示す解析方法に従って原因を切り分ける必要があります。

表 3-77　トラック状態が予想と異なる場合の対処方法

項番	確認内容・コマンド	対応
1	トラック情報の確認 • show track-object コマンドに <track-object id> パラメータを指定して，トラック情報を表示します。	表示されない場合またはトラック種別が UNSPECIFIED の場合は，トラックが設定されていません。 トラックの動作状態が無効状態 (Disable) の場合は，コンフィグレーションでトラックを停止しています。 コンフィグレーションを確認してください。
		トラックの動作状態が Init の場合は，起動直後のためトラックが動作を停止しています。起動待ち時間が経過するまでお待ちください。
		トラックが動作していて，かつトラック種別が ICMP の場合は項番 2 へ。
2	トラック対象と IPv4 通信ができるかどうかの確認 宛先アドレス，送信元アドレス，ネクストホップは，トラックの設定と同じ値を使用してください。 • ping コマンドを実行します。	ping の宛先アドレスと応答アドレスが異なる場合，該当アドレスは宛先アドレスのあるサブネットのブロードキャストアドレスです。 IPv4 ICMP ポーリング監視は，ブロードキャストアドレス宛てでは動作しません。 コンフィグレーションを確認してください。
		ネクストホップを指定していないトラックで，応答が戻らないまたは不安定である場合は，本装置とトラック対象装置の間の IPv4 ネットワークの通信を確認してください。
		ネクストホップを指定しているトラックで，応答が戻らないまたは不安定である場合は項番 3 へ。

項番	確認内容・コマンド	対応
3	ネクストホップに指定したルータと IPv4 通信ができるかどうかの確認 • ping コマンドを実行します。	ネクストホップに指定した装置との通信が不安定である場合は，本装置とネクストホップ装置との IPv4 ネットワークの通信を確認してください。
		ネクストホップに指定した装置との通信が安定している場合は，ネクストホップ装置とトラック対象装置との間の IPv4 ネットワークの通信を確認してください。

4 障害情報取得方法

この章では，主に障害情報取得作業を行うときの作業手順について説明しています。

4.1　保守情報の採取

装置の運用中に障害が発生した場合，ログ情報やダンプ情報が自動的に採取されます。また，運用コマンドを使用してダンプ情報を採取できます。

4.1.1　保守情報

IP8800/S4600 の保守情報を次の表に示します。ただし，スタック構成時，保守情報は各メンバスイッチにあります。そのため，スタック構成時は各メンバスイッチの情報を採取してください。

表 4-1　保守情報

<table>
<tr><th>項目</th><th>格納場所およびファイル名</th><th>備考</th></tr>
<tr><td>装置再起動時のダンプ情報ファイル</td><td>/dump0/rmdump</td><td rowspan="2">• ftp コマンドでファイル転送をする際はバイナリモードで実施してください。
• ファイル転送後は削除してください。</td></tr>
<tr><td>ネットワークインタフェース障害時のダンプ情報ファイル</td><td>/usr/var/hardware/ni00.000</td></tr>
<tr><td>ログ情報</td><td>採取したディレクトリから次の名前で格納します。
運用ログ：log.txt
種別ログ：log_ref.txt</td><td>• ftp コマンドでファイル転送をする際はアスキーモードで実施してください。</td></tr>
<tr><td>コンフィグレーションファイル障害時の情報</td><td>装置管理者モードで次のコマンドを実行し，二つのファイルをホームディレクトリにコピーします。その後，ファイル転送してください。
　cp /config/system.cnf system.cnf
　cp /config/system.txt system.txt
スタック構成時は各メンバスイッチのファイルをマスタスイッチにコピーしてください。
　cp switch <switch no.> /config/system.cnf system_<switch no.>.cnf
　cp switch <switch no.> /config/system.txt system_<switch no.>.txt</td><td>• ftp コマンドでファイル転送をする際はバイナリモードで実施してください。
• ファイル転送後はコピーしたファイルを削除してください。</td></tr>
<tr><td>障害待避情報</td><td>/usr/var/core/*.core</td><td>• ftp コマンドでファイル転送をする際はバイナリモードで実施してください。
• ファイル転送後は削除してください。</td></tr>
</table>

4.2　保守情報のファイル転送

この節では，ログ情報やダンプ情報をファイル転送する手順について説明します。

本装置の ftp コマンドを使用すると，保守情報をリモート運用端末やリモートホストにファイル転送できます。また，zmodem コマンドでコンソールにファイル転送することもできます。

スタック構成では，マスタスイッチからだけ保守情報のファイル転送ができます。マスタスイッチ以外のメンバスイッチの保守情報は，cp コマンドで各メンバスイッチからマスタスイッチにコピーしたあと，マスタスイッチからファイル転送をしてください。

4.2.1　ftp コマンドを使用したファイル転送

リモート運用端末との間でファイル転送を行う場合は ftp コマンドを使用します。

(1) ダンプファイルをリモート運用端末に転送する

図 4-1　ダンプファイルのリモート運用端末へのファイル転送

```
> cd ダンプ格納ディレクトリ                            <---1
> ftp 192.168.0.1                                      <---2
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt                                            <---3
Interactive mode off.
ftp> bin                                               <---4
200 Type set to I.
ftp>cd 転送先ディレクトリ                             <---5
250 CMD command successful.
ftp> put ダンプファイル名                             <---6
local: ダンプファイル名 remote: ダンプファイル名
200 EPRT command successful.
150 Opening BINARY mode data connection for 'ダンプファイル名'.
100% |*************************************|  3897       2.13 MB/s    00:00 ETA
226 Transfer complete.
3897 bytes sent in 00:00 (82.95 KB/s)
ftp> bye
221 Goodbye.
>
```

1. 転送元ディレクトリの指定
2. 転送先端末のアドレスを指定
3. 対話モードを変更
4. バイナリモードに設定※
5. 転送先ディレクトリの指定
6. ダンプファイルの転送

注※

ダンプファイルは必ずバイナリモードで転送してください。ダンプファイルをアスキーモードで転送すると，正確なダンプ情報が取得できなくなります。

(2) ログ情報をリモート運用端末に転送する

図 4-2 ログ情報のリモート運用端末へのファイル転送

```
> show logging > log.txt
> show logging reference > log_ref.txt
> ftp 192.168.0.1                                  <---1
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ascii                                         <---2
200 Type set to A.
ftp>cd 転送先ディレクトリ                           <---3
250 CMD command successful.
ftp> put log.txt                                   <---4
local: log.txt remote: log.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log.txt'.
100% |*************************************| 89019     807.09 KB/s    --:-- ETA
226 Transfer complete.
89019 bytes sent in 00:00 (315.22 KB/s)
ftp> put log_ref.txt
local: log_ref.txt remote: log_ref.txt
200 EPRT command successful.
150 Opening ASCII mode data connection for 'log_ref.txt'.
100% |*************************************|  4628       1.04 MB/s    --:-- ETA
226 Transfer complete.
4628 bytes sent in 00:00 (102.86 KB/s)
ftp> bye
221 Goodbye.
>
```

1. 転送先端末のアドレスを指定
2. アスキーモードに設定
3. 転送先ディレクトリの指定
4. ログ情報の転送

(3) 障害退避情報ファイルをリモート運用端末に転送する

図 4-3　障害退避情報ファイルのリモート運用端末へのファイル転送

```
> cd /usr/var/core/
> ls                                                   <---1
nimd.core       nodeInit.core
> ftp 192.168.0.1                                      <---2
Connected to 192.168.0.1.
220 FTP server (Version 6.00LS) ready.
Name (192.168.0.1:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> prompt                                            <---3
Interactive mode off.
ftp> bin                                               <---4
200 Type set to I.
ftp>cd 転送先ディレクトリ                               <---5
250 CMD command successful.
ftp> mput *.core                                       <---6
local: nimd.core remote: nimd.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'nimd.core'.
100% |*********************************************************************|
272 KB    1.12 MB/s    00:00 ETA
226 Transfer complete.
278528 bytes sent in 00:00 (884.85 KB/s)
local: nodeInit.core remote: nodeInit.core
200 EPRT command successful.
150 Opening BINARY mode data connection for 'nodeInit.core'.
100% |*********************************************************************|
1476 KB    1.40 MB/s    00:00 ETA
226 Transfer complete.
1511424 bytes sent in 00:01 (1.33 MB/s)
ftp> bye
221 Goodbye.
>
```

1. 障害退避情報ファイルが存在することを確認
   ファイルが存在しない場合は，何もせずに終了
2. 転送先端末のアドレスを指定
3. 対話モードを変更
4. バイナリモードに設定※
5. 転送先ディレクトリの指定
6. 障害退避情報ファイルの転送

注※

障害退避情報ファイルは必ずバイナリモードで転送してください。障害退避情報ファイルをアスキーモードで転送すると，正確な障害退避情報が取得できなくなります。

4.2.2　zmodem コマンドを使用したファイル転送

zmodem コマンドを使用して，本装置と RS232C ケーブルで接続されているコンソールとの間でファイル転送ができます。なお，通信を始めるに当たり，あらかじめコンソール側通信プログラムの受信操作を行ってください。

(1) ダンプファイルをコンソールに転送する

図 4-4 ダンプファイルのコンソールへのファイル転送

```
> cd ダンプ格納ディレクトリ                          <---1
> zmodem put ダンプファイル名                         <---2
>
```

1. 転送元ディレクトリの指定
2. ダンプファイルの転送

(2) ログ情報をコンソールに転送する

図 4-5 ログファイルのコンソールへのファイル転送

```
> show logging > log.txt
> show logging reference > log_ref.txt
> zmodem put log.txt                                    <---1
> zmodem put log_ref.txt
>
```

1. ログファイルの転送

(3) 障害退避情報ファイルをコンソールに転送する

図 4-6 障害退避情報ファイルのコンソールへのファイル転送

```
> cd /usr/var/core/
> ls                                                  <---1
interfaceControl.core    nodeInit.core
> zmodem put interfaceControl.core                    <---2
> zmodem put nodeInit.core
>
```

1. 障害退避情報ファイルが存在することを確認
   ファイルが存在しない場合は，何もしないで終了
2. ログファイルの転送

4.3　show tech-support コマンドによる情報採取とファイル転送

show tech-support コマンドを使用すると，障害発生時の情報を一括して採取できます。また，ftp パラメータを指定することで，採取した情報をリモート運用端末やリモートホストに転送できます。

スタック構成では，マスタスイッチで show tech-support コマンドを実行した場合だけ，ftp パラメータを指定したファイル転送ができます。マスタスイッチ以外のメンバスイッチに対しては，show tech-support コマンドで ftp パラメータを指定できません。

マスタスイッチ以外のメンバスイッチで show tech-support コマンドによる情報採取とファイル転送をする場合は，次の手順で実施してください。

1. マスタスイッチで次のコマンドを実行して，障害発生時の情報を採取します。
   `remote command <switch no.> show tech-support`
2. 各メンバスイッチで採取した情報を，cp コマンドで各メンバスイッチからマスタスイッチにコピーしたあと，マスタスイッチからファイル転送をします。
   ファイル転送をする手順は，「4.2　保守情報のファイル転送」を参照してください。

(1) show tech-support コマンドで情報を採取してファイル転送をする

図 4-7　保守情報のリモート運用端末へのファイル転送

```
> show tech-support ftp                                          <---1
Specify Host Name of FTP Server.       : 192.168.0.1             <---2
Specify User ID for FTP connections.   : staff1                  <---3
Specify Password for FTP connections.  :                         <---4
Specify Path Name on FTP Server.       : /usr/home/staff1        <---5
Specify File Name of log and Dump files: support                 <---6
Mon Dec 18 20:42:58 UTC 2006
Transferred support.txt .
Executing.
...............................................................................
...........
...............................................................................
........................................................
Operation normal end.
########## Dump files' Information ##########
***** ls -l /dump0 *****
total 2344
-rwxrwxrwx  1 root  wheel  2400114 Dec  8 16:46 rmdump
***** ls -l /usr/var/hardware *****
-rwxrwxrwx  1 root  wheel  264198 Dec  8 16:43 ni00.000
########## End of Dump files' Information ##########
########## Core files' Information ##########
***** ls -l /usr/var/core *****
No Core files
########## End of Core files' Information ##########
Transferred support.tgz .
Executing.
...............................................................................
...........
...............................................................................
........................................................
Operation normal end.
>
```

1. コマンドの実行

2. リモートホスト名を指定
3. ユーザ名を指定
4. パスワードを入力
5. 転送先ディレクトリの指定
6. ファイル名を指定

(2) remote command コマンドを使用して show tech-support コマンドで情報を採取する（スタック構成時）

図 4-8　メンバスイッチ（スイッチ番号 2）の保守情報をマスタスイッチに採取（スタック構成時）

```
> remote command 2 show tech-support > support.txt              <---1
Executing.
..............................................................................
...........
..............................................................................
......................................................
Operation normal end.
>
```

1. コマンドの実行

4.4　リモート運用端末の ftp コマンドによる情報採取とファイル転送

リモート運用端末やリモートサーバから ftp コマンドで本装置に接続し，ファイル名を指定することで，障害情報や保守情報を取得できます。

スタック構成では，ftp コマンドでマスタスイッチに接続できます。マスタスイッチ以外のメンバスイッチには，ftp コマンドで接続できません。

マスタスイッチ以外のメンバスイッチで障害情報や保守情報の採取とファイル転送をする場合は，次の手順で実施してください。

1. 各メンバスイッチで，障害情報や保守情報を採取します。
2. 各メンバスイッチで採取した情報を，cp コマンドで各メンバスイッチからマスタスイッチにコピーしたあと，マスタスイッチからファイル転送をします。
   ファイルを転送する手順は，「4.2　保守情報のファイル転送」を参照してください。

(1) show tech-support の情報を取得する

リモート運用端末をクライアントとして ftp コマンドで本装置に接続し，必要な show tech-support 情報のファイル名を指定して情報を取得する手順を次に示します。

表 4-2　ftp コマンドで取得できる情報

get 指定ファイル名	取得情報
.show-tech	show tech-support の表示結果
.show-tech-unicast	show tech-support unicast の表示結果
.show-tech-multicast	show tech-support multicast の表示結果
.show-tech-layer-2	show tech-support layer-2 の表示結果

図 4-9　show tech-support 基本情報の取得

```
client-host> ftp 192.168.0.60                      <---1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get .show-tech show-tech.txt                  <---2
local: show-tech.txt remote: .show-tech
150 Opening BINARY mode data connection for '/etc/ftpshowtech'.
226 Transfer complete.
270513 bytes received in 8.22 seconds (32.12 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
```

1. クライアントから本装置に ftp 接続
2. .show-tech ファイルをクライアントに転送（ファイル名は show-tech.txt を指定）

図 4-10 show tech-support **ユニキャスト情報の取得**

```
client-host> ftp 192.168.0.60                      <---1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> get .show-tech-unicast show-tech-uni.txt      <---2
local: show-tech-uni.txt remote: .show-tech-uni.txt
150 Opening BINARY mode data connection for '/etc/ftpshowtech'.
226 Transfer complete.
343044 bytes received in 30.43 seconds (11.01 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
```

1. クライアントから本装置に ftp 接続
2. .show-tech-unicast ファイルをクライアントに転送（ファイル名は show-tech-uni.txt を指定）

注

- ftp の ls などのコマンドで，get 指定すべきファイルは見えないので，事前のファイルの容量確認などはできません。
- 本情報の取得時は，装置側でコマンドを実行するため，転送中の状態が長く続きますが，途中で転送を中断しないでください。
- 装置の負荷状態や通信路の状態によっては，クライアント側がネットワークタイムアウトで切断することがあります。その場合は，クライアントのタイムアウト時間を長く設定してください。
- ftp での障害情報取得では show running-config コマンドなど，装置管理者モードでだけ実行できるコマンドの実行結果は採取しません。
- show tech-support を取得したときに，ログ情報に残るユーザ名は ftpuser となります。

(2) ダンプ情報ファイルを取得する

リモート運用端末をクライアントとして ftp コマンドで本装置に接続し，必要なダンプ情報のファイル名を指定して情報を取得する手順を次に示します。

表 4-3 ftp **コマンドで取得できるファイル**

get 指定ファイル名	取得ファイル
.dump	/dump0 と /usr/var/hardware 以下のファイル（圧縮）
.dump0	/dump0 以下のファイル（圧縮）
.hardware	/usr/var/hardware 以下のファイル（圧縮）

図 4-11 リモート運用端末からのダンプファイルの取得

```
client-host> ftp 192.168.0.60                          <---1
Connected to 192.168.0.60.
220 192.168.0.60 FTP server (NetBSD-ftpd) ready.
Name (192.168.0.60:staff1): staff1
331 Password required for staff1.
Password:
230 User staff1 logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> binary                                            <---2
200 Type set to I.
ftp> get .dump dump.tgz                                <---3
local: dump.tgz remote: .dump
150 Opening BINARY mode data connection for '/etc/ftpdump'.
226 Transfer complete.
2411332 bytes received in 5.78 seconds (407.13 KB/s)
ftp> quit
221 Thank you for using the FTP service on 192.168.0.60.
client-host>
```

1. クライアントから装置に ftp 接続
2. ダンプ情報ファイルは必ずバイナリモードで転送してください。
   アスキーモードでは転送できません。
3. .dump ファイルをクライアントに転送（ファイル名は dump.tgz を指定）

注

- ftp の ls などのコマンドで，get 指定すべきファイルは見えないので，事前のファイルの容量確認などはできません。
- 装置の負荷状態や通信路の状態によっては，クライアント側がネットワークタイムアウトで切断することがあります。その場合は，クライアントのタイムアウト時間を長く設定してください。

4.5 MC への書き込み

障害情報や保守情報は MC に書き込めます。ただし，MC の容量制限があるので注意してください。

4.5.1 運用端末による MC へのファイル書き込み

運用端末で装置の情報を MC に書き込みます。

図 4-12 MC **への情報書き込み**

```
書き込むためのMCを装置に挿入する。

ls -l コマンドでコピー元ファイル(tech.log)の容量を確認する。
> ls -l tech.log
-rw-r--r--  1 operator  users  234803 Dec 15 15:52 tech.log

show mcコマンドで空き容量を確認する。
>show mc
Date 20XX/12/15 15:50:40 UTC
MC  : Enabled
    Manufacture ID : 00000003
    16,735kB used
    106,224kB free                                 <---1
    122,959kB total

cpコマンドでコピー元ファイルをtech-1.logというファイル名称でMCにコピーする。
> cp tech.log mc-file tech-1.log

MCにファイルが書き込めていることを確認する。
> ls mc-dir
Name             Size
tech-1.log                234803
>
```

1. 空き容量

5 回線のテスト

5.1 回線をテストする

回線テストでは，テスト種別ごとに，テストフレームの折り返し位置が異なります。回線テスト種別ごとのフレームの折り返し位置を次の図に示します。

なお，スタック構成時の回線テストは未サポートです。

図 5-1 回線テスト種別ごとのフレームの折り返し位置

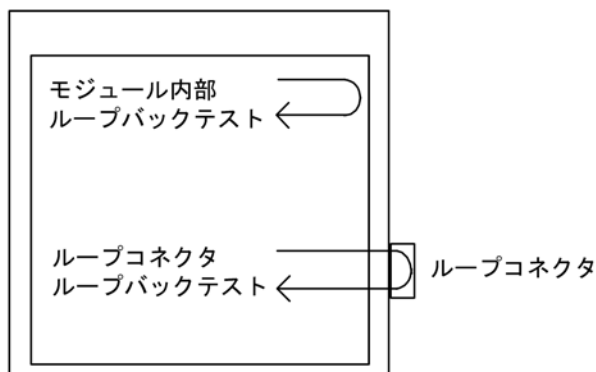



表 5-1 テスト種別と確認できる障害部位

テスト種別	フレームの折り返し位置	確認できる障害部位
モジュール内部 ループバックテスト	装置	NIF（RJ45 コネクタおよびトランシーバを除く）
ループコネクタ ループバックテスト	ループコネクタ	NIF（RJ45 コネクタおよびトランシーバ含む）

5.1.1 モジュール内部ループバックテスト

モジュール内部ループバックテストは装置内でフレームを折り返し，障害の有無を確認します。このテストはすべての回線種別で実行できます。

テストの手順を次に示します。

1. inactivate コマンドでテスト対象のポートを inactive 状態にします。
2. test interfaces コマンドに internal パラメータを指定し実行します。その後，約 1 分間待ちます。
3. no test interfaces コマンドを実行し，表示される結果を確認します。
4. activate コマンドでポートを active 状態に戻します。

NIF 番号 1，ポート番号 1 に対し，テストフレームの送信間隔を 2 秒に設定してテストした例を次の図に示します。

図 5-2 モジュール内部ループバックテストの例

```
> inactivate gigabitethernet 1/1
> test interfaces gigabitethernet 1/1 internal interval 2 pattern 4

> no test interfaces gigabitethernet 1/1
Date 20XX/12/20 00:20:21 UTC
Interface type            :100BASE-TX
Test count                :30
Send-OK                   :30             Send-NG                 :0
Receive-OK                :30             Receive-NG              :0
Data compare error        :0              Out underrun            :0
Out buffer hunt error     :0              Out line error          :0
In CRC error              :0              In frame alignment      :0
In monitor time out       :0              In line error           :0
H/W error                 :none
> activate gigabitethernet 1/1
```

テストを実施後，次のことを確認してください。

”Send-NG”および”Receive-NG”が 0 の場合，回線テスト結果は正常です。

”Send-NG”および”Receive-NG”が 0 でない場合は，何らかの異常があります。マニュアル「運用コマンドレファレンス」の，no test interfaces コマンドの表示内容を参照してください。

5.1.2 ループコネクタループバックテスト

ループコネクタループバックテストはループコネクタでフレームを折り返し，障害の有無を確認します。このテストはすべての回線種別で実行できます。

テストの手順を次に示します。

1. inactivate コマンドでテスト対象のポートを inactive 状態にします。
2. 対象ポートのケーブルを抜き，ループコネクタを接続します※。
3. test interfaces コマンドに connector パラメータを指定して実行します。その後，約 1 分間待ちます。
4. no test interfaces コマンドを実行し，表示される結果を確認します。
5. ループコネクタを外し，ケーブルを元に戻します。
6. activate コマンドでポートを active 状態に戻します。

注※

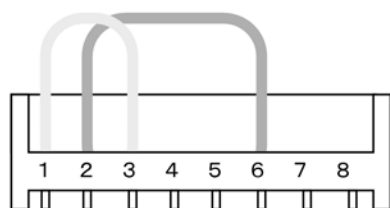
ループコネクタが未接続の場合，またはそのポートに対応したループコネクタが接続されていない場合，正しくテストができないので注意してください。

なお，テストの実行結果は「5.1.1 モジュール内部ループバックテスト」と同様に確認してください。

5.1.3 ループコネクタの配線仕様

(1) 10BASE-T/100BASE-TX 用ループコネクタ

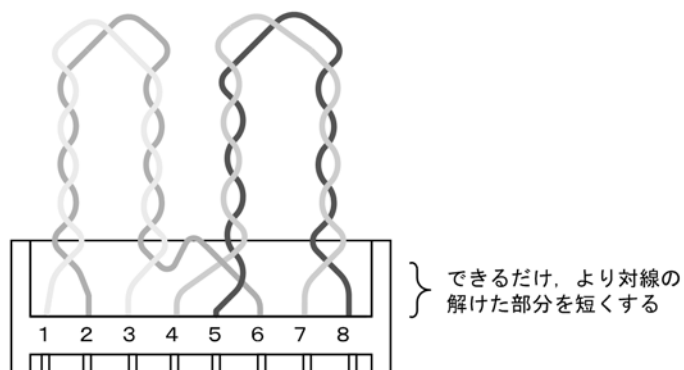
次の図のように，ケーブルをコネクタに差込み，圧着工具で圧着します。

図 5-3 10BASE-T/100BASE-TX **用ループコネクタの配線仕様**

(2) 10BASE-T/100BASE-TX/1000BASE-T 用ループコネクタ

1. あらかじめ 6 ～ 7cm の 2 本のより対線を作ります。

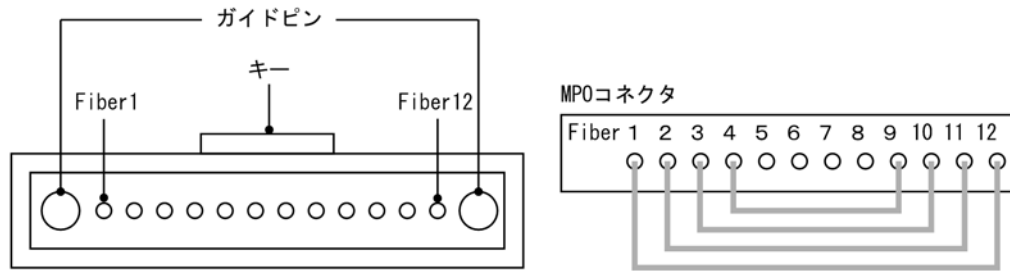
図 5-4 より対線

2. 次の図のように，ケーブルをコネクタに差込み，圧着工具で圧着します。

図 5-5 10BASE-T/100BASE-TX/1000BASE-T **用ループコネクタの配線仕様**

なお，上記ループコネクタでの 1000BASE-T のループ動作は，本装置だけで動作を保証します（1000BASE-T のコネクタを使用するループ動作は，規格上規定されていない独自動作です）。

(3) 40GBASE-SR4 用ループコネクタ

次の図のような配線仕様のループコネクタを使用してください。

図 5-6　40GBASE-SR4 **用ループコネクタの配線仕様**

6 装置の再起動

この章では，主に装置を再起動する場合の作業手順について説明します。

6.1　装置を再起動する

6.1.1　装置の再起動

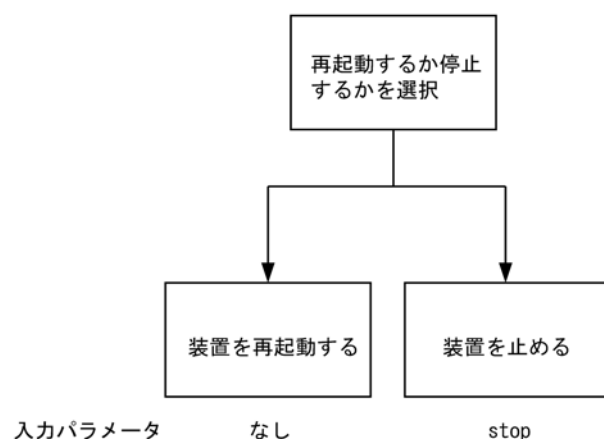
reload コマンドを使用して，装置を再起動できます。また，再起動時にログを保存します。

コマンドの入力形式，パラメータについてはマニュアル「運用コマンドレファレンス」を参照してください。

実行例として，「装置を再起動」し，CPU メモリダンプ採取については確認メッセージに従って行う場合の，reload コマンドのパラメータ選択について説明します。

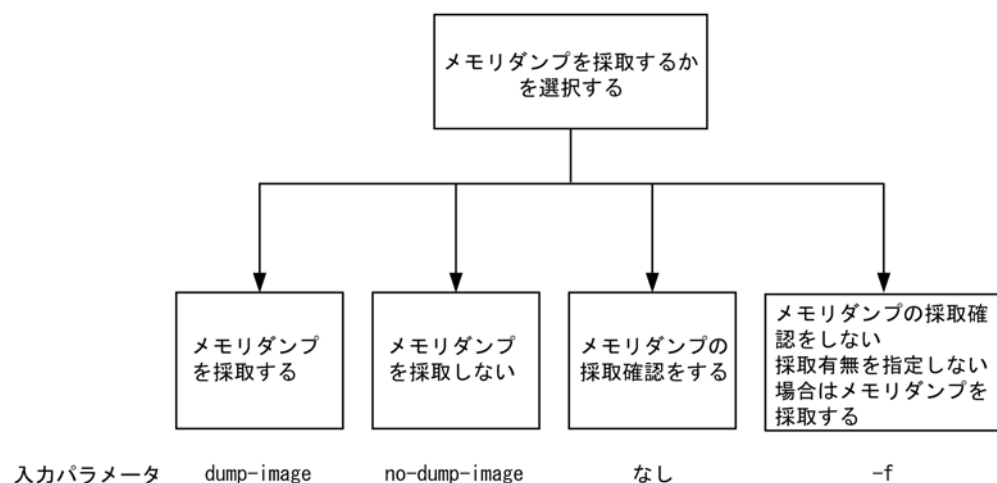
Step1

装置を再起動するか，停止するかを選択します。

図 6-1　装置再起動・停止選択

Step1 では，装置を再起動させるので，上記の図によりパラメータは選択しません。

Step2

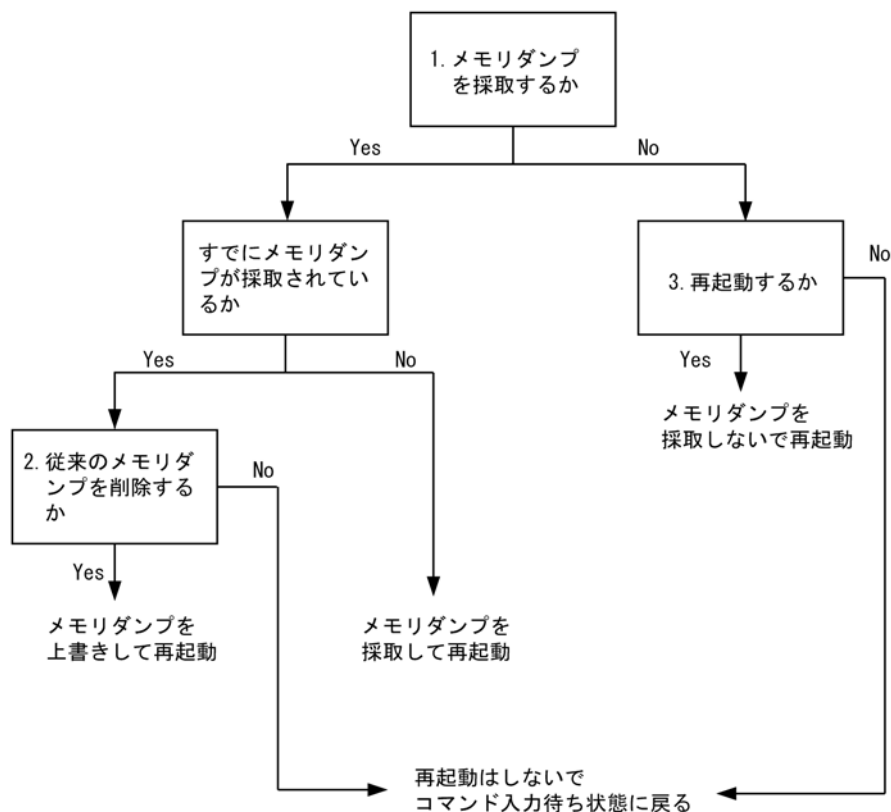
次にダンプ採取するかどうかを選択します。

図 6-2　CPU メモリダンプ採取選択

Step2 では，CPU メモリダンプ採取の確認をするので，上記の図によりパラメータは選択しません。Step1 から Step2 で選択したパラメータを組み合わせると「reload」となります。このコマンドを入力すると，以下のような，ダンプ採取確認メッセージが出力されます。

1. Dump information extracted?(y/n):_
2. old dump file(rmdump 01/01 00:00) delete OK? (y/n):_
3. Restart OK? (y/n):_

上記のメッセージが出力されるタイミングは，次に示すフローチャートの番号に対応しています。

図 6-3　CPU メモリダンプ採取確認メッセージ

付録

付録 A　show tech-support コマンド表示内容詳細

付録 A.1　show tech-support コマンド表示内容詳細

show tech-support コマンドでプロトコルのパラメータ指定ごとに表示されるコマンドの内容を次の表に示します。

なお，表示内容の詳細については，マニュアル「運用コマンドレファレンス」を参照してください。

【注意】

show tech-support コマンドで表示される情報の一部については，マニュアル「運用コマンドレファレンス」に記載しておりません。これらの情報は装置の内部情報を含んでいるため非開示としております。
また，ソフトウェアバージョンによって一部表示されるものとされないものがあります。あらかじめご了承ください。

表 A-1　表示内容詳細

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
1	show version	本装置のソフトウェアバージョン情報およびハードウェア情報	○	○	○	○
2	show license	オプションライセンス情報	○	○	○	○
3	show system	装置の運用状態	○	○	○	○
4	show environment	ファン / 電源 / 稼働時間情報	○	○	○	○
5	show process cpu	プロセスの CPU 使用情報	○	○	○	○
6	show process memory	プロセスのメモリ使用情報	○	○	○	○
7	show cpu days hours minutes seconds	CPU 使用率	○	○	○	○
8	show memory summary	装置のメモリ使用情報	○	○	○	○
9	/sbin/dmesg	カーネル内イベント情報	○	○	○	○
10	cat /var/run/dmesg.boot	カーネル内イベント情報	○	○	○	○
11	cat /var/log/messages	カーネルおよびデーモンの内部情報	○	○	○	○
12	/usr/local/diag/statShow	カーネル内部統計情報	○	○	○	○
13	/usr/local/diag/pk_tmrd	稼働時間情報	○	○	○	○
14	fstat	ファイルデスクリプタ情報	○	○	○	○
15	/usr/local/diag/rtsystat	内部デバイス関連情報	○	○	○	○
16	/usr/local/diag/rtastat	経路配布関連情報	○	○	○	○
17	show netstat all-protocol-address numeric	レイヤ 4 関連統計情報	○	○	○	○
18	show netstat statistics	レイヤ 3 関連統計情報	○	○	○	○
19	show dumpfile	採取済みのダンプファイル情報	○	○	○	○
20	ls -lTiR /dump0	ダンプファイル情報	○	○	○	○
21	ls -lTiR /usr/var/hardware	ハードウェアダンプファイル情報	○	○	○	○
22	ls -lTiR /usr/var/core	core ファイル情報	○	○	○	○

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
23	ls -lTiR /config	config ファイル情報	○	○	○	○
24	ls -lTiR /var	メモリファイルシステム情報	○	○	○	○
25	df -ik	パーティション情報	○	○	○	○
26	du -Pk /	ファイルシステム使用状況	○	○	○	○
27	show logging	運用系時系列ログ情報	○	○	○	○
28	show logging reference	運用系種別ログ情報	○	○	○	○
29	show ntp associations	ntp サーバの動作情報	○	○	○	○
30	/usr/bin/w -n	ログイン関連情報	○	○	○	○
31	show session	ログインセッション情報	○	○	○	○
32	/usr/sbin/pstat -t	端末情報	○	○	○	○
33	stty -a -f /dev/tty00	コンソール端末情報	○	○	○	○
34	cat /var/log/clitrace1	CLI トレース情報 1	○	○	○	○
35	cat /var/log/clitrace2	CLI トレース情報 2	○	○	○	○
36	cat /var/log/mmitrace	運用コマンドトレース情報	○	○	○	○
37	cat /var/log/kern.log	カーネル内部トレース情報	○	○	○	○
38	cat /var/log/daemon.log	デーモン関連内部トレース情報	○	○	○	○
39	cat /var/log/fixsb.log	カーネル内部トレース情報	○	○	○	○
40	cat /usr/var/pplog/ppupdate.log	ソフトウェアアップデート実行時のログ情報	○	○	○	○
41	cat /usr/var/pplog/ppupdate2.log	ソフトウェアアップデート実行時のログ情報	○	○	○	○
42	tail -n 30 /var/log/authlog	認証トレース情報	○	○	○	○
43	tail -n 30 /var/log/xferlog	FTP トレース情報	○	○	○	○
44	cat /var/log/ssh.log	SSH ログ情報	○	○	○	○
45	show accounting	アカウンティング情報	○	○	○	○
46	cat /var/tmp/gen/trace/mng.trc	コンフィグレーションコマンドトレース情報 1	○	○	○	○
47	tail -n 20 /var/tmp/gen/trace/api.trc	コンフィグレーションコマンドトレース情報 2	○	○	○	○
48	cat /var/tmp/gen/trace/mng_sub.trc	コンフィグレーションコマンドトレース情報 3	○	○	○	○
49	tail -n 400 /var/tmp/gen/trace/ctl.trc	コンフィグレーションコマンドトレース情報 5	○	○	○	○
50	show netstat interface	カーネル内インタフェース情報	○	○	○	○
51	show ip-dual interface	IPv4/IPv6 インタフェースの状態	○	○	○	○
52	show vlan list	VLAN 情報一覧	○	○	○	○
53	show port	ポートの情報	○	○	○	○
54	show port statistics	ポートの統計情報	○	○	○	○
55	show port protocol	ポートのプロトコル情報	○	○	○	○

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
56	show port transceiver debug	ポートのトランシーバ詳細情報	○	○	○	○
57	show interfaces nif XXX_NIF line XXX_LINE debug	ポートの詳細統計情報	○	○	○	○
58	show power inline	PoE 情報	○	○	○	○
59	show switch detail	スタックの詳細情報	○	○	○	○
60	show running-config	運用面のコンフィグレーション	○	○	○	○
61	show channel-group detail	リンクアグリゲーションの詳細情報	○	○	○	○
62	show spanning-tree detail	スパニングツリーの詳細情報	○	○	○	○
63	show gsrp all	すべての GSRP 詳細情報	○	○	○	○
64	show axrp detail	Ring Protocol の詳細情報	○	○	○	○
65	show switchport-backup detail	アップリンクリダンダントの詳細情報	×	×	×	○
66	show switchport-backup statistics	アップリンクリダンダントの統計情報	×	×	×	○
67	show efmoam detail	IEEE802.3ah/OAM 機能の設定情報およびポートの状態	○	○	○	○
68	show efmoam statistics	IEEE802.3ah/OAM 機能の統計情報	○	○	○	○
69	show lldp detail	LLDP 機能の隣接装置情報	○	○	○	○
70	show oadp detail	OADP 機能の隣接装置情報	○	○	○	○
71	show loop-detection	L2 ループ検知機能の情報	×	×	×	○
72	show loop-detection statistics	L2 ループ検知機能の統計情報	×	×	×	○
73	show loop-detection logging	L2 ループ検知機能のログ情報	×	×	×	○
74	show channel-group statistics	リンクアグリゲーション統計情報	×	×	×	○
75	show channel-group statistics lacp	リンクアグリゲーションの LACP 統計情報	×	×	×	○
76	show spanning-tree statistics	スパニングツリーの統計情報	×	×	×	○
77	show vlan detail	VLAN 情報詳細	×	○	○	○
78	show vlan mac-vlan	MAC VLAN 情報	×	×	×	○
79	show qos queueing	全キューの統計情報	○	○	○	○
80	show ip cache policy	ポリシーベースルーティングの状態表示	○	○	○	○
81	policy tool tech	ポリシーベースプログラムの内部トレース	○	○	○	○
82	show access-filter	フィルタ機能の統計情報	×	○	○	○
83	show qos-flow	QoS 制御機能の統計情報	×	○	○	○
84	show lldp statistics	LLDP 機能の統計情報	×	×	×	○
85	show oadp statistics	OADP 機能の統計情報	×	×	×	○
86	show mac-address-table	mac-address-table 情報	×	○	○	○

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
87	show dot1x logging	IEEE802.1X 認証で採取した動作ログメッセージ	×	×	×	○
88	show dot1x statistics	IEEE802.1X 認証に関わる統計情報	×	×	×	○
89	show dot1x detail	IEEE802.X 認証に関わる認証状態情報	×	×	×	○
90	show igmp-snooping	IGMP snooping 情報	×	×	×	○
91	show igmp-snooping group	IGMP snooping のグループ情報	×	×	×	○
92	show igmp-snooping statistics	IGMP snooping の統計情報	×	×	×	○
93	show mld-snooping	MLD snooping 情報	×	×	×	○
94	show mld-snooping group	MLD snooping のグループ情報	×	×	×	○
95	show mld-snooping statistics	MLD snooping の統計情報	×	×	×	○
96	show netstat routing-table numeric	カーネル内経路関連情報（ユニキャスト）	×	○	○	×
97	show netstat multicast numeric	カーネル内経路関連情報（マルチキャスト）	×	×	○	×
98	show ip multicast statistics	IPv4 マルチキャスト統計情報	×	×	○	×
99	show ipv6 multicast statistics	IPv6 マルチキャスト統計情報	×	×	○	×
100	show ip multicast resources	IPv4 マルチキャストルーティングで使用している各エントリ数	×	×	○	×
101	show ip igmp interface	IGMP が動作するインタフェース情報	×	×	○	×
102	show ip igmp group	IGMP が管理するグループ情報	×	×	○	×
103	show ip pim interface (detail)	IPv4 PIM が動作するインタフェース情報	×	×	○	×
104	show ip pim neighbor (detail)	IPv4 PIM の近隣情報	×	×	○	×
105	show ip pim bsr	IPv4 PIM の BSR 情報	×	×	○	×
106	show ip pim rp-mapping	IPv4 PIM のランデブーポイント情報	×	×	○	×
107	show ip mroute	IPv4 マルチキャスト経路情報	×	×	○	×
108	show ip mcache	IPv4 マルチキャスト中継エントリ	×	×	○	×
109	show ipv6 multicast resources	IPv6 マルチキャストルーティングで使用している各エントリ数	×	×	○	×
110	show ipv6 mld interface	MLD が動作するインタフェース情報	×	×	○	×
111	show ipv6 mld group	MLD が管理するグループ情報	×	×	○	×
112	show ipv6 pim interface (detail)	IPv6 PIM が動作するインタフェース情報	×	×	○	×
113	show ipv6 pim neighbor (detail)	IPv6 PIM の近隣情報	×	×	○	×
114	show ipv6 pim bsr	IPv6 PIM の BSR 情報	×	×	○	×
115	show ipv6 pim rp-mapping	IPv6 PIM のランデブーポイント情報	×	×	○	×
116	show ipv6 mroute	IPv6 マルチキャスト経路情報	×	×	○	×

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
117	show ipv6 mcache	IPv6 マルチキャスト中継エントリ	×	×	○	×
118	show ip multicast statistics	IPv4 マルチキャスト統計情報	×	×	○	×
119	show ipv6 multicast statistics	IPv6 マルチキャスト統計情報	×	×	○	×
120	show vrrpstatus detail statistics	VRRP の仮想ルータの状態と統計情報	×	○	×	×
121	show track detail	VRRP の障害監視インタフェース情報	×	○	×	×
122	show ip interface ipv4-unicast	ユニキャストルーティングプログラムが認識している本装置のインタフェース情報	×	○	×	×
123	show processes memory unicast	ユニキャストルーティングプログラムでのメモリの確保状況および使用状況	×	○	×	×
124	show processes cpu minutes unicast	ユニキャストルーティングプログラムの CPU 使用率	×	○	×	×
125	show dhcp giaddr all	DHCP リレーエージェントの DHCP パケットの受信先 IP アドレス情報	×	○	×	×
126	show dhcp traffic	DHCP リレーエージェント統計情報	×	○	×	×
127	show ip dhcp server statistics	DHCP サーバ統計情報	×	○	×	×
128	show ip dhcp conflict	DHCP サーバ衝突 IP アドレス情報	×	○	×	×
129	show ipv6 dhcp server statistics	IPv6 DHCP サーバ統計情報	×	○	×	×
130	show ipv6 dhcp traffic	IPv6 DHCP リレー統計情報	×	○	×	×
131	show ip dhcp snooping statistics	DHCP snooping 統計情報	○	○	○	○
132	show ip arp inspection statistics	ダイナミック ARP 検査統計情報	○	○	○	○
133	show ip dhcp snooping logging info	DHCP snooping ログ情報	×	×	×	○
134	dhsn debug	DHCP snooping イベント情報	×	×	×	○
135	show ip route summary	ルーティングプロトコルが保有するアクティブ経路数と非アクティブ経路数	○	○	○	○
136	show ip rip statistics	RIP の統計情報	×	○	×	×
137	show ip rip advertised-routes summary	RIP で広告した経路数	×	○	×	×
138	show ip rip received-routes summary	RIP で学習した経路数	×	○	×	×
139	show ip ospf	OSPF のグローバル情報	×	○	×	×
140	show ip ospf discard-packets	OSPF で廃棄されたパケット情報	×	○	×	×
141	show ip ospf statistics	OSPF で収集されている送受信パケットの統計情報	×	○	×	×
142	show ip ospf neighbor detail	OSPF の隣接ルータの詳細情報	×	○	×	×
143	show ip ospf virtual-links detail	OSPF の仮想リンク情報の詳細情報	×	○	×	×
144	show ip ospf database database-summary	OSPF の LS タイプごとの LSA 数	×	○	×	×

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
145	show ip bgp neighbor detail	BGP4 のピアリング情報	×	○	×	×
146	show ip bgp notification-factor	BGP4 のコネクションを切断する要因となったメッセージ	×	○	×	×
147	show ip bgp received-routes summary	BGP4 のピアから受信した経路情報数	×	○	×	×
148	show ip bgp advertised-routes summary	BGP4 のピアへ広告した経路情報数	×	○	×	×
149	show ip vrf all	各種 VRF の学習経路数	○	○	○	○
150	show ipv6 interface ipv6-unicast	ユニキャストルーティングプログラムが認識している本装置のインタフェース情報	×	○	×	×
151	show ipv6 route summary	ユニキャストルーティングプログラムが保有するアクティブ経路数と非アクティブ経路数	○	○	○	○
152	show ipv6 rip advertised-routes summary	RIPng で広告した経路数	×	○	×	×
153	show ipv6 rip received-routes summary	RIPng で学習した経路数	×	○	×	×
154	show ipv6 rip statistics	RIPng の統計情報	×	○	×	×
155	show ipv6 ospf	OSPFv3 のグローバル情報	×	○	×	×
156	show ipv6 ospf discard-packets	OSPFv3 で廃棄されたパケットの情報	×	○	×	×
157	show ipv6 ospf statistics	OSPFv3 で収集したパケットの統計情報	×	○	×	×
158	show ipv6 ospf neighbor detail	OSPFv3 の隣接ルータの状態	×	○	×	×
159	show ipv6 ospf virtual-links detail	OSPFv3 の仮想リンク情報	×	○	×	×
160	show ipv6 ospf database database-summary	OSPFv3 の LS-Database の数	×	○	×	×
161	show ipv6 bgp neighbor detail	BGP4+ のピアリング情報	×	○	×	×
162	show ipv6 bgp notification-factor	BGP4+ のコネクションを切断する要因となったパケット	×	○	×	×
163	show ipv6 bgp received-routes summary	BGP4+ のピアから受信した経路情報数	×	○	×	×
164	show ipv6 bgp advertised-routes summary	BGP4+ のピアへ広告した経路情報数	×	○	×	×
165	show ipv6 vrf all	各種 VRF の学習経路数	○	○	○	○
166	show web-authentication user edit	内蔵 Web 認証 DB への登録・変更内容の表示	×	×	×	○
167	show web-authentication user commit	内蔵 Web 認証 DB の登録内容の表示	×	×	×	○
168	show web-authentication statistics	Web 認証の統計情報の表示	×	×	×	○
169	show web-authentication login	認証済のユーザ情報（アカウント情報）の表示	×	×	×	○

項番	コマンド（表示）	内容	パラメータ指定なし	unicast	multicast	layer-2
170	show web-authentication logging	Web 認証の動作ログの表示	×	×	×	○
171	show sflow detail	sFlow 統計情報（詳細）の表示	○	○	○	○
172	port snd/rcv statistics	ポート送受信統計情報	○	○	○	○
173	internal SW HW event statistics0	内部 SW イベント統計情報 0	○	○	○	○
174	internal SW HW event statistics1	内部 SW イベント統計情報 1	○	○	○	○
175	show mac-authentication	MAC 認証の設定情報の表示	×	×	×	○
176	show mac-authentication statistics	MAC 認証の統計情報の表示	×	×	×	○
177	show mac-authentication mac-address edit	内蔵 MAC 認証 DB への登録・変更内容の表示	×	×	×	○
178	show mac-authentication mac-address commit	内蔵 MAC 認証 DB の登録内容の表示	×	×	×	○
179	show mac-authentication login	認証済のユーザ情報（アカウント情報）の表示	×	×	×	○
180	show mac-authentication logging	MAC 認証の動作ログの表示	×	×	×	○
181	show power-control schedule	省電力機能のスケジュール表示	○	○	○	○
182	swdev logging	SW 部ログの表示	○	○	○	○
183	SW MMU statistics0	SW 部 MMU 統計情報 0	○	○	○	○
184	spc port statistics	SPC 統計情報	○	○	○	○
185	show environment temperature-logging	温度履歴情報	○	○	○	○
186	show track-object detail	ポリシーベースルーティングのトラッキング機能情報詳細	○	○	○	○
187	/usr/local/bin/trackobj -t | tail -n 1024	ポリシーベースルーティングのトラッキング機能トレース情報	○	○	○	○
188	/usr/local/bin/fdbmerge_show -s	MAC アドレステーブル同期機能情報	○	○	○	○
189	/usr/local/bin/fdbmerge_show	MAC アドレステーブル同期機能詳細情報	×	×	×	○
190	show vxlan	VXLAN インタフェース情報	×	×	×	○
191	show vxlan vni	VXLAN VNI 情報	×	×	×	○
192	show vxlan peers	VXLAN VTEP のピア情報	×	×	×	○
193	show vxlan mac-address-table	VXLAN MAC アドレステーブル情報	×	×	×	○

（凡例）　○：表示対象　×：非表示対象
注　コマンド（表示）列の（　）は，ソフトウェアのバージョンによっては表示されることを示しています。

索引

数字

A

B

C

D

F

G

I

L

M

N

O

R

S

V

W

Z

い

う

え

か

き

こ

し

す

そ

つ

と

ね

ふ

ほ

も

り

る

れ

ろ